2018

Cyber Threats and Healthcare Organizations: A Public Health Preparedness Perspective

Lauren Elizabeth Branch
West Virginia University, lbranch@mix.wvu.edu

Cyber Threats and Healthcare Organizations: A Public Health Preparedness Perspective

Lauren E. Branch, MPH

Dissertation submitted to the School of Public Health at West Virginia University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Occupational and Environmental Health Sciences

Tom Bias, Ph.D., Chair
Warren Eller, Ph.D., Mentor
Michael McCawley, Ph.D.
Douglas Myers, Sc.D.
Brian Gerber, Ph.D.

Department of Occupational and Environmental Health Sciences

Morgantown, West Virginia
2018

Key Words: Cyberattack, Healthcare, Malware, Trends, Threat, Ransomware, Hospitals, United States

Abstract

Cyber Threats and Healthcare Organizations: A Public Health Preparedness Perspective

Lauren E. Branch

Healthcare in the United States, heavily reliant on digital technology in service provision, has recently seen an increase risk of cyberattacks. Coordinated electronic medical records, imaging, pharmaceutical services, lab services and even treatment devices all rely on electronic connectivity and represent critical services that must be secured from cyberthreats. Hospitals have become increasingly complex systems, and this often makes the organization more vulnerable to failure. Planning for these events is often hard for hospitals because their main charge is to provide life-saving care to patients as they need it. This is a relatively new threat to healthcare organizations, and there has not been limited research on this hazard and its impacts on healthcare organizations.

Therefore, the aim of the first study was to assess the trend of successful major malware attacks on healthcare organizations in the United States between 2016 and 2017. Previous research found limited research specific to malware attacks and found most articles covering ransomware were restricted to news articles. A content analysis was conducted on articles from two well-renowned health IT organizations. This study identified 49 attack cases across 27 states. Based on previously reported statistics, the number of identified cases was low meaning healthcare organizations are not reporting their attacks. A true risk assessment cannot be completed by the industry until a more representative trend analysis can be completed.

The aim of the second study was to assess the organizational outcomes of a malware attack on a healthcare organization. Previous research on this health hazard discussed healthcare's lack of preparedness for this new threat but did not delve in to the organization's response, mitigation, and recovery from attacks. Therefore, qualitative interviews were conducted with key stakeholders from three organizations that suffered malware attacks during the years 2016-2017. Topics covered were system impact, system recovery and business continuity, and changes to organizational preparedness efforts. One of the main findings from this study was the realization by health stakeholders how connected their organization, and therefore the provision of care, has become. Participants also discussed their lack of full understanding on the potential impact these attacks could have on their organizations before their attack, including the loss of every digital system within their facility. A need was expressed across all facilities that more information about these attacks need to become shared across the industry to better prepare organizations and protect patient safety.

The final aim of the final study was to examine organizational preparedness efforts and to identify the organizational barriers to mitigating the threats arising from cyberattacks. A survey was conducted among healthcare emergency mangers to assess their perceptions of preparedness for cyber threats. While the majority of respondents reported feeling either confident or very confident in both their individual and their organizational ability to respond to a cyber attack, their responses regarding preparedness actions their organization has taken against cyber threats were lacking. When it comes to events like ransomware, where attack impacts are still not fully understood, the healthcare industry remains less prepared.

In conclusion, these studies indicate a need for data related to cyberattacks to be collected in a central repository that is either made public or shared among healthcare stakeholders. In order to best prepare their organizations, there needs to be accurate risk assessments completed and areas for preparedness with the best return on investment can then be identified. Cyberattacks are only expected to increase over the next five years. Patient care is put at risk during each of these attacks and it is essential for healthcare organizations to be better prepared for this new hazard to keep the organization's patients, workers, and community safe.

Dedication

This dissertation is dedicated to the memory of my Dad, William R. Branch. Losing you was the hardest thing I have ever had to endure, and to have lost you suddenly in the beginning of this program was devastating. I pushed myself to continue and have finally finished in your honor. It's funny that my dissertation topic ended up being something related to your line of work. I wish more than anything we could go to lunch and discuss it all. I have come to realize how many characteristics we shared; you truly helped shape the woman I have become. I was lucky to have such a loving, generous, funny, intelligent and thoughtful person for a Dad. I am so grateful for the years we had together, and I will cherish our memories always. You were my sounding board for life and my best friend. I strive every day to make you proud and to carry on your legacy. "For never before in story or rhyme (not even once upon a time) has the world ever known a you, my friend, and it never will, not ever again…"

I would also like to dedicate this work to my Mom, Patty L. Branch, who is both my biggest fan and the #1 Mountaineer Fan. There are not enough words to express my gratefulness for everything you have done to make this dream a possibility. Thank you for always listening to me anytime, day or night, offering sage advice throughout this process (even when you had no idea what I was talking about), and pushing me to be the best I can be. Your encouragement, thoughtfulness, and friendship are things I will always be thankful for. You have been my constant cheerleader and savior. Without your support I could not have made it through the last four years, both in this program and in life.

Finally, I would like to thank Carson and Brody, my two red-headed, furry brothers. They have endured many hugs, tears, and joy from me over the years, and hopefully this degree will help them understand why I always had to leave them to go back to school. All my love!

Acknowledgements

First and foremost, I would like to thank my committee members, Dr. Warren Eller, Dr. Tom Bias, Dr. Doug Myers, Dr. Michael McCawley, and Dr. Brian Gerber, for providing me with guidance throughout this process and insightful feedback. Dr. Eller has supported me for the past 6 years throughout my graduate school experience and cultivated my interest in emergency preparedness and policy research. Dr. Bias has been so generous to jump on board towards the end of this process and help shepherd me through to the finish line. Dr. Myers and Dr. McCawley, my two OEHS mentors and professors, have always taught me to think critically and ask the hard questions when human safety and health are on the line. I will always be grateful for the knowledge they imparted on me in all of their courses and throughout my research. Dr. Gerber was gracious enough to join my early morning meetings from a different time zone, as well as provide me with helpful emergency management insight. In addition to my committee, I have had a few other mentors throughout this program. I want to thank Bobbi Sykes for your amazing and unwavering support. I could always count on your ear, your advice, and your kindness. I truly would not be where I am today without you. Dr. Lindsay Allen, thank you for allowing me to be your teaching assistant and for helping me shape my passions in to lectures. I will always be thankful for my time with you. Dr. Ranjita Misra, thank you for the experience of working with you on grants and on the accreditation project. I am truly grateful to have had those experiences. I would also like to thank my fellow graduate students for helping me get through this program. The years have not always been easy, but you all made it enjoyable.

I was lucky enough to also have mentors within the applied world, Dr. Lee Smith and Roger Osbourn. I would like to thank them for their guidance and support throughout this degree, as well as their expert knowledge related to my research area. Without them I would be lost on my path. I also want to sincerely thank both the Monongalia County Health Department and the Safety Department at WVU Medicine for the opportunities they provided me. I will always be incredibly thankful for my experiences and I will never forget the lessons I have learned from my time there.

I would also like to thank the rest of my family and friends. To my extended family, Aunt Sharon, Margaret and family, Uncle Don, Aunt Chris, Ollie and Josh, DeAnna and family, and Cara Beth- I cannot thank you enough. I am beyond grateful to have each and every one of you in my life. Thank you for always making me feel loved and supported; I would not be where I am today without you. A special thank you to Susan Fox for your generosity, kindness, and assistance throughout school. Fred Sievers, thank you for your patience while I finished this monster and for your mentorship. Thank you to Lisa Houlihan, Michelle Cavanaugh, Morgan Vandenberge, Tina Cowan, and Kayla Younciak, all of whom made life fun and this process bearable. Last but not least, thank you, thank you, thank you to my clan of strong, smart, independent, and beautiful sisters, Kate Siegrist, PhD, Katie Wilson, JD, MA, Rachel Morgenstern, MPA, Veronica Milliken Boggs, MS, and Katie Moore, MA.

Finally, I would like to sincerely thank the four hospitals and the hospital association who participated in this research project and wish to remain anonymous. Without your incomparable knowledge and invaluable insights this research project truly would not have been possible. You all are a part of the amazing group of devoted Emergency Managers and Public Health Professionals that exist across the country. You are the true heroes who remain steadfast in your dedication to serving the public and keeping them safe despite constant work pressures and funding cuts.

Table of Contents

I. Introduction

Organizations today face a myriad of hazards they must prepare for to ensure a safe environment for clients, employees, and to ensure business continuity. These hazards can range from a facility threat such as fire or loss of power, to a safety threat such as an active shooter. To better prepare for these threats and to coordinate a more efficient response, organizations develop emergency operating procedures. Cybercrime is a new and emerging threat that must be considered when preparing an institution's emergency operating procedures.

One specific industry that is particularly vulnerable to cybercrime is the healthcare industry due to their reliance on electronic health information, as well as their outdated security systems (Luna, Rhine, Myhra, Sullivan, & Krise, 2016). Coordinated electronic medical records, imaging, pharmaceutical services, lab services and even treatment devices all rely on electronic connectivity and represent critical services that must be secured from cyber threats. An even newer threat to healthcare organizations are malware attacks, where cybercriminals can encrypt an organization's files, essentially shutting that organization off electronically. Beginning in 2016, there has been a string of ransomware attacks on hospitals across the United States.

In May 2017, there was an outbreak of more than 75,000 ransomware attacks that targeted at least 99 countries around the globe, which experts are calling one of the biggest cybersecurity incidents they have seen (Larson, 2017). As part of this attack, at least 36 healthcare organizations across Great Britain were locked out of their computer systems causing the National Health Service to cancel outpatient appointments and divert patients away from emergency departments (Perlroth & Sanger, 2017). In December 2017, a Homeland Security advisor said this attack and its effects directly put lives at risk (Chappell & Neuman, 2017).

Not only does this threat put patients' health at risk, but these attacks cost the United States healthcare system an exorbitant amount of money. In 2015 alone, the FBI received 2,500 complaints of ransomware attacks across all industries, which cost the victims $214 million (Radke, Waters, Cleary, Evans, & Kittle, 2016). An American Public Health Association publication cited a technology report which said in 2016 there were 1,500 cyberattacks on health-related organizations that exposed personal information on over 155 million Americans. This publication also noted that the cost of healthcare data breaches is highest across all industries (Krisberg, 2017).

Very few studies have examined ransomware attacks, and how they could potentially affect healthcare organizations. A systematic review published in 2016, found only 19 articles published in peer-reviewed journals between 2008 and 2015 on the topic, and the majority of these focused on data breaches of protected health information (Luna et al., 2016). It is essential to understand the risk, mitigation, and preparedness of this threat to protect the safety of those within and of those served by the hospital (Ayala, 2016). There is a need to catalog the existing cyber threats hospitals face and to expand their knowledge of organizational preparedness and mitigation of these threats.

Background

Environmental Health is tasked with making the natural or built environment a safer place for those utilizing it (Healthy People 2020, 2017). Healthy People 2020 highlighted disaster preparedness as an emerging issue in the field of Environmental Health (Healthy People 2020, 2017). Within this area, the Centers for Disease Control and Prevention has an Office of Public Health Preparedness and Response, which is "committed to strengthening the nation's health security by protecting against public health threats, whether they begin at home or abroad, or if they are natural or man-made" (Centers for Disease Control and Prevention, 2017).

This paper serves as a public health preparedness exploration of the new and emerging cyber threats to healthcare organizations within the United States. Its defined environment is that of the hospital, and the cyber threats hospitals now face is the new threat to the safety of those within this environment.

Hospital safety

Patient safety and quality of care are two ways that hospitals are evaluated on environmental safety. The Agency for Healthcare Research and Quality (AHRQ), part of the United States Department of Health and Human Services, is tasked with producing evidence to help improve the safety and quality of healthcare services (AHRQ, 2016). The Centers for Medicare and Medicaid Services (CMS) use evidence put forth by AHRQ to help set quality goals and enforces these goals with their healthcare providers (Centers for Medicare and Medicaid Services, 2016). The Joint Commission is another group that works to improve patient safety and quality of care. This is a non-profit accreditation group for hospitals, which evaluates patient safety and quality of care before giving a hospital the 'golden seal of approval'. This accreditation earned by hospitals shows that the facility is committed to providing safe and high quality care to all its patients (The Joint Commission, 2017).

Even though organizations like The Occupational Safety and Health Administration (OSHA) and Joint Commission work to ensure a safe environment for both patients and employees, an emergency or disaster situation can drastically change a facility's day-to-day operations. Disasters often require healthcare workers to put in long hours, which puts them at an increased risk of injury (Dembe, Erikson, Delbos, & Banks, 2005). To help ensure hospitals' ability to both respond to hazards effectively and to continue to provide a safe environment of care for patients and staff, there are certain regulatory requirements in place specific to emergency management. First, The Joint Commission provides a chapter of standards specific

to Emergency Management, which a hospital must meet to be eligible for accreditation. Under the first requirement hospitals must conduct a hazard vulnerability assessment to see what hazards their hospital may have to deal with. The next requirement is that the hospital must have a written Emergency Operating Procedures (EOP) that addresses communications, resources, safety, staff, utilities, and patient care. The final requirement is that healthcare facilities must exercise their EOP twice a year to make sure their plan is current and viable (The Joint Commission E-dition, 2016). The Centers for Medicare and Medicaid Services has also developed new requirements for Emergency Management in healthcare. The new standards were released in September of 2016 and became effective on November 15, 2016. This new ruling states that the existing regulations are insufficient in ensuring a healthcare facility will be able to provide for their community during times of disaster (Medicare and Medicaid Programs, 2016). The community served by hospitals includes not only patients, families, and visitors, but workers as well (Cagliuso, 2014a). The ruling focuses on three essential areas: 'safeguarding human resources, maintaining business continuity, and protecting physical resources. The ruling addresses all parts of the disaster cycle: prepare, respond, mitigate, and recover. Qualified providers much develop a new emergency preparedness program to include a thorough risk assessment, plans and policies that address hazards identified in the risk assessment, training and exercising of the plans and polices, and an additional communication plan to allow for two-way communication between providers and their employees (See Figure 1). The goal of this CMS ruling is to enhance healthcare facilities' ability to continue providing care to their served community during times of disasters.

Cybercrime and cyberterrorism on the rise

Over the past 30 years, cybercrime and cyberterrorism have grown from potential concern to common threat. Cyber threats became a national security issue following Y2K and 9/11 (Stohl, 2007). After the terrorist attacks on 9/11, President Bush created the Office of

Cyberspace Security to be managed by Richard Clarke (Weimann, 2005). In this position, Clarke continued to raise the issue of a potential cybersecurity attack on various United States targets (Stohl, 2007). There was also a special congressional commission created after the attack on 9/11 to examine terrorism risks to the United States. This commission was concerned with the potential use of a cyberattack in conjunction with a regular terrorist attack (Weimann, 2005).

Often, the terms used to define cyberattacks are used interchangeably when they have different meanings. Denning (2000) defines Cyberterrorism as "the convergence of cyberspace and terrorism". This means for an act to be classified as cyberterrorism, it must have a cyber aspect, as well as have the motivation to create fear or coercion on a government or a specific population (Weimann, 2005). Potential targets for cyberterrorism exist among the United States infrastructure, including the nation's financial network, any type of traffic control including air and train travel, electrical grids or dams, and water-treatment plants (Squitieri, 2002). There are also fears that terrorists could use a cyberattack in concert with a traditional terrorist attack to hinder the rescue efforts taking place (Weimann, 2005; Squitieri, 2002). There are aspects of cyberterrorism that may make it more appealing to terrorists than traditional terror attacks. First, cyberterrorism is conducted remotely, making it easier for the perpetrators to remain anonymous. Second, cyberattacks are much cheaper than traditional terror attacks. Finally, the reach and potential impact that terrorists have with cyberattacks is far greater than with traditional terror attacks (Weimann, 2005).

Cybercrime is defined as an unlawful act in which a computer may be the tool and/or the victim (Dashora, 2011). According to the FBI, billions of dollars are spent each year repairing systems that have been affected by cybercrime. One of the major targets of cybercrime is data, particularly identifiable data, including identities, bank accounts, and electronic medical records (EMRs). In 2006, it was estimated that identity theft costs U.S. business over $50 billion with an

additional $5 billion in expenses to individuals (Kshetri, 2009). A study by the Ponemon Institute saw a 19% rise in cybercrime in 2015 (Gordon, 2016). Along with the rising trend of cybercrimes, these kinds of attacks are becoming more complex and far reaching.

One of the most notorious cyberattacks in 2016 was the hacking that took place during the U.S. Presidential Election. Russian hackers leaked confidential emails and documents from both the Democratic National Committee and the Democratic Congressional Campaign Committee. It has also become apparent since the election that Russia had a hand in trying to influence who became President of the United States (Lipton, Sanger, & Shane, 2016). In 2016, President Obama said that the United States has the potential to be more vulnerable than other nations to cyberattacks because of the large size of the U.S. economy and because of the high amount of digitization in this country (Kelly, 2016).

In March of 2018, the Department of Homeland Security and the Federal Bureau of Investigations released a joint statement regarding Russian hacking of critical United States infrastructure (Naylor, 2018). Some targets of Russian hacking include nuclear power plants, our electrical energy sector, and commercial facilities. The statement states the U.S. Intelligence Community has known about Russian hackings in the U.S. since at least March of 2016. In the summer of 2016, Russia launched a 'multi-stage intrusion campaign' against U.S. utilities, and an outcome of this attack was hackers gained access to at least one power plant's control system. In 2015, Russian hackers disrupted power to more than 200,000 people in Ukraine when they hacked a power plant and shut down services (Naylor, 2018). A New York Times article claims that Russia has been targeting U.S. and European critical infrastructure, including water treatment facilities, since 2015. This same article also discusses claims from private security firms that these coordinated attacks have been occurring since 2013 (Perlroth & Sanger, 2018).

One specific cybercrime is a ransomware attack, which has become much more common against organizations (Larson, 2017). There was a 159% jump seen in ransomware attacks from March to April of 2016. The normal increase between months had previously been only 9-20% (Lee, 2016 May). The FBI says that in 2016, there were 2,673 victims of ransomware attacks across the United States.

Attacks of this kind have been seen on many different types of organizations, including government/municipalities, education, churches, law enforcement, commercial businesses, and even the healthcare sector. During late 2017 to early 2018, three counties in North Carolina were targeted and attacked. In December 2017, Mecklenberg County, NC was the victim of a foreign-based hacker who gained access to the system by using a government employee's log-in information. When county officials made it clear they would not pay the $23,000 ransom, hackers made more attempts to get further in to the system (Douglas & Harrison, 2017). In February 2018, Davidson County was attacked and all county systems, including phone systems, were affected. This attack directly compromised the county's 911 Emergency Communication System (Hightower, 2018). These threats pose a direct risk to public health emergency preparedness (Barnett, Snell, Lord, Jenkins, Terbush, & Burke, 2013).

Two major ransomware attacks, WannaCry and NotPetya, occurred within a month of each other in the summer of 2017 and had effects seen around the globe. The WannaCry attack took place in May 2017, and infected computers in 150 countries. This attack has since been linked to North Korea (Nakashima, 2018). The other major attack was the NotPetya attack, in June of 2017, which has since been linked to Russia (Nakashima, 2018). The NotPetya virus infected computers in Denmark, India, and the United States, but most of its victims were located in Ukraine. This virus mocked a ransomware virus while it was in fact permanently deleting files. A few affected organizations were banks, energy companies, an airport, and government officials. One U.S. company that was affected was the pharmaceutical

company, Merck. Employees were said to be sent home from all U.S. plants during this attack, and a report on the impact of the attack said Merck revenue went down $135 million due to lost sales (Davis, 2017).

According to a 2016 Justice Department Report, on average in 2016 there were up to 4,000 ransomware attack attempts a day. This was a 300% increase from the average number of daily attacks seen in 2015. Ransomware is no longer a threat of a future, but rather one that all organizations must take seriously.

Hospitals role during disasters

According to the American Hospital Association (AHA), there were 5,534 registered hospitals in the United States at the start of 2018. These hospitals serve as major medical care providers for their communities, providing emergency services, outpatient visits, surgeries, and births. In 2015, the AHA states 142 million individuals were treated in U.S. emergency departments, and there were 581 million outpatient visits at U.S. hospitals in the same year (American Hospital Association, 2017). The AHA touts U.S. hospitals as also being economic anchors for their communities. They provide employment for more than 5.7 million individuals, and purchase almost $852 billion in goods and services from other businesses (American Hospital Association, 2017).

Hospitals also serve as a major component of the Nation's disaster response framework (Barnett et al., 2013). Shutting healthcare providers down via cyberattack would hinder our Nation's response ability to any type of disaster, natural or manmade, and could seriously impair the ability to protect public health. In the event of an emergency, hospitals will be responsible for handling a patient surge and for providing care to any and all that need it (Barbera, Yates, & Macintyre, 2009; Sauer, McCarthy, Knebel, & Brewster, 2009). As part of the National Response Framework, there were 15 Emergency Support Functions (ESF) identified for

disaster response. These ESFs provide a structure for the Federal response to any emergency. Each of these functions provides support, services, and resources for the specific need during a response. Healthcare services during disaster response falls into ESF-8, Public Health and Medical Services, and the services that fall under ESF-8 include medical care personnel, medical equipment, hospital care, and outpatient care (Office of the Assistant Secretary for Preparedness and Response, 2015).

Prior to 9/11, hospitals' main emergency management concern were both physical threats to the facility itself, such as a flood or tornado, and the patient surge caused during a community emergency (Center for Biosecurity of UPMC, 2009). After 9/11, the way our country viewed emergency preparedness changed drastically. President George W. Bush created the Department of Homeland Security to create a more coordinated effort in preparing for terrorist attacks. To create the Department of Homeland Security, 22 Federal agencies and departments were pulled under the DHS umbrella. After the creation of the DHS, the President issued different Homeland Security Presidential Directives (HSPD) to better define policies related to national security. Many of these directives were related to preparedness within the health care system. HSPD-8, issued in 2003, clearly defines hospitals as emergency response providers (Sauer et al., 2009). This means that hospitals must provide for the medical needs of the community during a disaster. In 2004, HSPD-10 was issued in response to bioterrorism fears. This directive says that hospitals must be prepared for all hazards, including explosives and bioterrorist attacks.

The Department of Health and Human Services (DHHS) also plays a large role in emergency response for public health and medical care. Specific to hospitals is the Hospital Preparedness Program (HPP), which was created under DHHS in 2002 to prepare hospitals for bioterrorism and pandemic flu (Center for Biosecurity of UPMC, 2009). This program was originally administered by the Health Resources and Services Administration (HRSA) branch of

DHHS. In the wake of Hurricane Katrina, the Pandemic and All-Hazards Preparedness Act (PAHPA) was passed to help our nation better prepare for and be better at responding to disasters (Office of the Assistant Secretary for Preparedness and Response, 2017). With the passing of the PAHPA in 2006, Congress created the Office of the Assistant Secretary for Preparedness and Response (ASPR) and directed the HPP to be shifted from HRSA to ASPR. Currently, the HPP is still run through ASPR to provide funding for hospital emergency preparedness efforts. This funding program is a way to ensure hospitals meet certain response capabilities defined by the federal government (Sauer et al., 2009). The goal of the HPP is to improve community response coordination and to strengthen healthcare resources and tools available for medical emergency response.

The Joint Commission requires hospitals to conduct a risk assessment of their facility once per year (Marx & Slonim, 2003). This risk assessment will prioritize certain threats to the facility, and show what areas the hospital needs to focus on with their preparedness efforts. Hospitals have become increasingly complex systems, and this complexity often makes the organization more vulnerable to failures and attacks (Morton, 2011). Low probability high impact events normally occur without much warning. Planning for these types of events is often hard for hospitals because their main charge is to provide life-saving care to patients as they need it. Hospitals are generally more concerned with high probability low impact events, such as medical errors and patient safety, rather than cyberattacks.

One hospital tool that is critical to help manage patient surge during disasters is the electronic medical record. Not only do hospital staff need quick access to patient records as the patient is admitted for care, but electronic medical records also provide a way to track disaster patients throughout the emergency. The different cyber risks healthcare providers now face threaten to diminish their ability to provide critical care during times of emergency.

Cyber terror: Is the US healthcare system safe?

Amid growing threats of cyberattacks in the United States, it is important for hospitals to be better prepared to prevent a successful attack. Some of the cyber threats facing the healthcare industry include data breaches and malware viruses. With the shift to electronic medical records (EMRs), cybersecurity within healthcare first began as an important issue regarding Health Insurance Portability and Accountability Act (HIPAA) compliance (Perakslis, 2014). HIPAA requires safeguards be put in place to ensure privacy and protection of sensitive information (Luna et al., 2016). Another important piece of legislation regarding privacy and EMRs is the Health Information Technology for Economic and Clinical Health (HITECH) Act. This Act increased funding for health information technology to further "meaningful use" through technology like EMRs, which was a term created by CMS. The goal of "meaningful use" was to improve quality, safety, and efficiency of care, to reduce disparities, and to improve coordination of care by allowing patient care information to have a central storage where all providers could access data and care history (See Figure 2). The Centers for Medicare and Medicaid Services developed the EHR Incentive Program which offered payments as an incentive for providers to both purchase EHRs and to demonstrate "meaningful use" with patient care. The goal of the incentive was improvement of population health. The EMR Incentive Program increased the use of certified health IT, and in 2016 around 96% of hospitals across the country were using EMRs (Figure 3). This increased use brings about a larger need for privacy protection (Barnett et al., 2013; Kruse, Frederick, Jacobson, & Monticone, 2017).

Although data privacy is a priority for healthcare providers, breaches in patient information still occur. According to Department of Health and Human Services (DHHS) breach database, in October 2015, over 163,000 individual health records were breached. The Office of Civil Rights within DHHS claims that over 113 million medical records were breached in 2015. A recent study published in The Journal of the American Medical Associated performed a

content analysis on breach data from the DHHS database between the years 2010 and 2017 (McCoy and Perlis, 2018). The study found that healthcare providers have seen an increase in data breaches since the passing of the HITECH Act in 2009 (See Figure 4). In 2017, healthcare providers reported 37.2 million cumulative records being breached. There are different causes of data breaches, including theft, loss, improper disposal, and hacking/IT incident. The authors of the JAMA study separated the data out by breach type (See Figure 5). Breaches due to hacking/IT incidents have steadily increased since 2010 but saw a spike since 2015. The number of breaches due to hacking or IT incident almost doubled between 2015 and 2016. In 2017, data breach by hacking/IT incident because the number one breach type in healthcare.

Threats like malware and ransomware are relatively new to the healthcare industry. A systematic review published in 2017 showed that the healthcare industry is less prepared for cyber security issues than other industries (Kruse et al., 2017). With regard to cyber threats, hospitals take precautions with data privacy, including training all staff on HIPAA policy, because they are cautious of repercussions to any violations. But when it comes to events like ransomware, where attacks used to be considered rare, the organization as a whole is less prepared. There has been a more recent push for hospitals by groups like Joint Commission to prepare for low probability high impact events, events that are less likely to happen but could have a larger impact on the organization.

During ransomware attacks, hackers will use malware to lock the computers within a network and demand a ransom payment for the decryption code. These kinds of attacks essentially shut down the hospital's ability to operate electronically and can potentially affect patient care. The major global attack in May of 2017 that locked 36 health organizations out of their systems in Great Britain was said to have a directly put patients' lives at risk (Chappell & Neuman, 2017).

Due to their inherent nature, hospitals make perfect targets for ransomware attacks. They depend on up to date patient records and health data to provide critical care to their patients. Approximately 95% of hospitals use health information technology, including electronic medical records (Luna et al., 2016). These electronic records hold essential information, such as medication needs and patient care directives, and may be needed at a moment's notice. Malware attacks would lock out access to these records and put patient safety at risk.

This type of attack is a new cyber-threat for hospitals, and therefore many organizations have out of date cybersecurity systems and have not trained staff on security awareness. Many hospitals focus on training staff to be HIPAA compliant because of the data privacy pressures, and fail to train them on how to keep the organization's system safe as a whole (Zetter, 2016). One of the main routes of entry for malware viruses are through phishing attacks. These attacks will send an email to members of the organization with a malicious link or attachment, and once an individual clicks on the link or opens the attachment the virus has a way in to the network.

Another factor that makes hospitals a perfect target for ransomware attacks is their status as a business. Over time hospitals have evolved from providing a social service for their local communities to becoming a business tasked with making a profit (Barbera et al., 2009, Cagliuso, 2014a). If a ransomware attack shuts down the hospital's ability to care for patients, the hackers are also stopping the hospital from making their profit. Making a small ransom payment might be seen as the most beneficial solution to hospital executives, so that hospital staff can get back to work and continue to see patients.

Timeline of hospital attacks

An outbreak of ransomware attacks on hospitals began in February of 2016 at the Hollywood Presbyterian Medical Center in Los Angeles, California. The hospital was negatively

impacted for days and eventually decided to pay the ransom. After their computers were offline for over a week, the ransom payment was made for approximately $17,000 and the hospital regained access to its systems. Since this initial attack in the healthcare field, there has been a large increase in reported ransomware attacks across hospitals in the United States.

These attacks within the United States were not the only ones seen on healthcare organizations since 2016. There were also ransomware attacks seen on hospitals in Canada and Great Britain (Chappell & Neuman, 2017, Lee, 2016 Mar; Chung, 2016). There are different reports on how often this is occurring to healthcare organizations, but there has not been a report created on successful attacks. The risk reports that do exist also don't expound on the nature and scope of these attacks. Some of these attacks are affecting just a few computers within organizations, while other attacks are significantly impacting the organization's ability to provide patient care. Due to the initial payment of the Los Angeles Hospital and the inherent nature of hospitals, these types of attacks are only believed to continue to grow in frequency.

Gaps in Literature

Cybersecurity has been a research topic of concern for quite some time (Stohl, 2007; Weimann, 2005). However, this topic was discussed more as a potential concern that should be considered when developing threat preparedness plans (Squitieri, 2002). It wasn't until more recently, when these concerns started coming to fruition, that there was an increase in the healthcare literature (Dashora, 2011). The JAMA Article discussed above summarized data breaches using the DHHS data portal including breaches by hacking, however the data lacks any other type of cyber threats facing healthcare and is limited to a data breach as the outcome.

A search of the literature found two systematic reviews published on this topic since 2016, both completed by Texas State University (Kruse et al., 2017; Luna et al., 2016). The first

review found 19 articles related to this topic of cybersecurity and healthcare (Luna et al., 2016). This review identified threat types, discussed in the literature, including data breaches, internal and external threats, cyber-squatting, and cyberterrorism. The reviewers noted that data breaches were the most common cyber threat to healthcare. Only one of their 19 identified articles discussed Denial of Service attacks on healthcare, but there was no mention of ransomware in this review. The second review focused more on the modern threats healthcare faces in cybersecurity (Kruse et al., 2017). The review included 'ransomware' as a search criterion, which was not included in the first systematic review. This search returned 31 articles that were analyzed. One of the themes the authors saw in their article review was that cyber threats to healthcare organizations are growing, and there is a systematic lack of preparedness seen across this industry sector. One of the limitations of this review the authors noted was many of the articles returned were from news sources and not from peer-review publications. They attribute this to ransomware being such a new threat to healthcare organizations.

Another topic covered in the literature is information technology (IT) solutions to cybersecurity issues. This literature lives in the IT world, using IT language to span the vast array of cybersecurity threats. The articles discuss potential end points or ways in to a system, as well as potential solutions or patches to stop anyone getting in to a system. One research article pointed out that much of the literature covers IT's role during cyber emergencies, and how IT departments are tasked with getting systems back up and running after an attack (Barnett et al., 2013).

From a public health and a threat preparedness perspective, the literature identifies cyber threats as a problem for the healthcare industry, but the research does not delve much deeper in to the topic. One article which links cyber threats directly to public health states the exact effects on public health, as well as potential mitigation strategies against this type of threat is lacking from the literature (Barnett et al., 2013). This research project hopes to better define

the threat of ransomware against healthcare, to identify some best practices of organizations that have faced attacks and to identify barriers to cyber-preparedness within healthcare organizations. A more robust understanding of cyber threats against hospitals is needed to help identify areas for preparedness action and would ultimately make it possible to improve cybersecurity preparedness in the healthcare industry. A hospital environment that is more secure against cyber threats is a safer environment for patients, workers, and the community at large.

Purpose of the Research

This study is meant to serve as a descriptive, exploratory study of a new and emerging threat to healthcare organizations in this country. The objective of this project is to assess trends in malware attacks against healthcare, to examine organizational best practices to mitigate the effects of and to re-establish business continuity after a malware attack, and to expand their knowledge of organizational preparedness and mitigation of these threats. To achieve the study objective, I will pursue the following three specific aims.

Specific Aim 1:

To assess the trend of successful major malware attacks on healthcare organizations in the United States between 2016 and 2017. A content analysis will be conducted on web articles related to malware and hospitals to create a summary of successful and publicly reported attacks beginning with the 2016 outbreak. A logic diagram will be created through identifying technological assets within a hospital that are vulnerable to cyberattack and could, if compromised during such an attack, jeopardized patient safety through interviews with key informants.

Specific Aim 2:

To assess the organizational outcomes of a malware attack on a healthcare organization. Interviews will be conducted with key stakeholders in healthcare cybersecurity to compare outcomes from three facilities that were victims of malware attacks. Interview subjects included representatives from healthcare IT, emergency management, and administration. Key evaluation questions for interviews will be identified based on existing literature and conversations with subject matter experts to assess the impact of a successful malware attack on a healthcare organization.

Specific Aim 3:

To examine organizational preparedness efforts and to identify the organizational barriers to mitigating the threats arising from cyberattacks. A survey will be conducted on safety, emergency management, and information technology staff from a healthcare organization on their perceptions and knowledge of their organization's preparedness for cyber threats. The survey will be created based on existing literature and interviews with key stakeholders to assess the barriers to an organization's readiness for cyber threats.

This research is significant because it will expand on the knowledge of cyberattacks against healthcare organizations, as well as provide novel data on ransomware attacks within the healthcare industry. Completion of this research will provide an understanding of cyber vulnerabilities within a hospital and identify what happens to hospitals during malware attacks. The results will also preparedness actions hospitals are taking and highlight barriers to becoming more prepared for these threats.

The novel data provided by this research project will allow hospital's to be more informed when making organizational decisions on emergency preparedness and mitigation. First,

having more detailed information regarding a specific threat category against the healthcare industry will allow for a more accurate representation of cyber threats within the organizational hazard vulnerability assessment (HVA). The HVA is required by The Joint Commission and Centers for Medicare and Medicaid Services to ensure a hospital's ability to continue serving their community (Centers for Medicare and Medicaid Services, 2018; The Joint Commission E-dition, 2016). A well-informed assessment is the foundation for good preparedness efforts and the key to a successful response. Second, CMS and The Joint Commission also require healthcare organizations to review and update their emergency plans annually to ensure continuity of operations and provision of patient care. The CMS Emergency Preparedness Rule even requires an emergency plan to cover interruptions to communications, including from cyber attack (CMS, 2018). In order to effectively meet these requirements from regulatory agencies and be prepared to ensure continuity of operations during an incident, healthcare needs to have a better understanding of the risk these threats pose to their operations and provision of care. Hospitals and healthcare providers serve as a building block in our Nation's disaster response framework (Barnett et al., 2013). If there is an emergency or disaster in our country, hospitals are tasked with providing care to all that need it (Barbera et al., 2009; Sauer et al., 2009). The healthcare industry is facing this new threat they need a more comprehensive understanding of to prepare their organizations and to ensure they can remain a cornerstone in our country's response network.

References

Agency for Healthcare Research and Quality. (2016 Dec). Quality and patient safety. Retrieved from https://www.ahrq.gov/professionals/quality-patient-safety/index.html

American Hospital Association (2018). Fast facts on U.S. hospitals, 2018. Retrieved from https://www.aha.org/statistics/fast-facts-us-hospitals

American Hospital Association (2017). Hospitals are economic anchors in their communities. Retrieved from https://www.aha.org/statistics/2018-03-29-hospitals-are-economic-anchors-their-communities

American Hospital Association (2013). Cyber security and hospitals: Four questions every hospital leader should ask in order to prepare for and manage cybersecurity risks. Retrieved from https://www.aha.org/system/files/2017-12/ahaprimer-cyberandhosp.pdf

Ayala, L. (2016). Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention. Berkely: Apress.

Barbera, J.A., Yeatts, D.J., & Macintyre, A.G. (2009). Challenge of hospital preparedness: analysis and recommendations. *Disaster Med Pub Health Prep*, 3(S1), S74-82.

Barnett, D.J., Snell, T.K., Lord, R.K., Jenkins, C.J., Terbush, J.W., & Burke, T.A. (2013). Cyber security threats to public health. *World Med Health Policy*, 5(1), 37-46.

Becker's Hospital Review (2016, Jun 1) 93% of phishing emails contain ransomware. *Becker's Hospital Review,* Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/93-of-phishing-emails-contain-ransomware.html

Cagliuso, N. V. (2014a). Stakeholders' experiences with US hospital emergency preparedness: Part 1. *J Bus Contin Emer Plan*, 8(2), 156-168.

Center for Biosecurity of UPMC. (2009). Hospitals rising to the challenge: the first five years of the U.S. hospital preparedness program and priorities going forward. Retrieved from http://www.upmchealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2009/2009-04-16-hppreport.pdf

Centers for Disease Control and Prevention. (2017). Office of Public Health Preparedness and Response. Retrieved from https://www.cdc.gov/phpr/index.htm

Centers for Medicare and Medicaid Services. (2018). Core EP rule elements. Retrieved from https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Core-EP-Rule-Elements.html

Centers for Medicare and Medicaid Services. (2016). CMS quality strategy. Retrieved from https://www.cms.gov/medicare/quality-initiatives-patient-assessment-instruments/qualityinitiativesgeninfo/downloads/cms-quality-strategy.pdf

Chappell, B. and Neuman, S. (2017, Dec 19). U.S. says North Korea 'directly responsible' for wannacry ransomware attack. *NPR*. Retrieved from https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

Chung, E. (2016, Mar 24). Ontario hospital website may have infected visitors with ransomware, security firm says. *CBC News*. Retrieved from http://www.cbc.ca/news/technology/norfolk-general-hospital-hack-1.3504229

Dashora, K. (2011). Cyber crime in the society: problems and preventions. *J Alt Persp Soc Sci*, 3(1), 240-259.

Davis, J. (2017, Oct 27). Petya cyberattack cost Merck $135 million in revenue. *Healthcare IT News*. Retrieved from http://www.healthcareitnews.com/news/petya-cyberattack-cost-merck-135-million-revenue

Dembe, A.E., Erikson, J.B., Delbos, R.G., & Banks, S.M. (2005). The impact of overtime and long work hours on occupational injuries and illnesses: new evidence from the United States. *Occup Environ Med*, 62, 588-597.

Department of Health and Human Services. Top 10 tips for cybersecurity in health care. Retrieved from https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

Douglas, A. and Harrison, S. (2017, Dec 8). After North Carolina county refuses to pay hacker ransom, attackers strike again. *Government Technology*, Retrieved from http://www.govtech.com/network/After-North-Carolina-County-Refuses-to-Pay-Hacker-Ransom-Attackers-Strike-Again.html

Gordon, P. (2016, Aug 25). Rise of the cyber criminals. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/entry/rise-of-the-cyber-criminals_us_57bed90ae4b06384eb3e60b9

Healthcare IT News & HIMSS Analytics. Healthcare IT News and HIMSS Analytics quick HIT survey: Ransomware, 2016. Retrieved from https://healthmanagement.org/c/it/news/ransomware-attacks-hit-three-quarters-of-hospitals-without-them-knowing

Healthy People 2020. (2017). Environmental Health. Retrieved from https://www.healthypeople.gov/2020/topics-objectives/topic/environmental-health

Hightower, D. (2018, Feb 21). Davidson County, N.C., still reeling from ransomware attack. *Government Technology*, Retrieved from http://www.govtech.com/security/Davidson-County-NC-Still-Reeling-from-Ransomware-Attack.html

Justice Department. (2016, Jun). How to protect your networks from ransomware: interagency technical guidance document. Retrieved from https://www.justice.gov/criminal-ccips/file/872771/download

Kelly, M.L. (2016, Dec 16). Obama: espionage is being 'turbocharged' by the internet. *NPR*. Retrieved from http://www.npr.org/sections/parallels/2016/12/16/505864712/obama-espionage-is-being-turbocharged-by-the-internet

Krisberg, K. (2017). Cybersecurity: Public health increasingly facing threats. *The Nation's Health,* 107 (8), 1195.

Kruse, C.S., Frederick, B., Jacobson, T., & Monticone, D.K. (2017). Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care,* 25, 1-10.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Commun ACM*, 52(12). 141-144.

Larson, S. (2017, May 13). Massive cyberattack targeting 99 countries causes sweeping havoc. *CNN Tech*, Retrieved from http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html

Lee, S. (2016, May 3). Ransomware attacks reached record high in April- and aren't slowing down: report. *Newsweek*. Retrieved from http://www.newsweek.com/ransomware-attacks-reached-record-high-april-and-not-slowing-down-report-455239)

Lee, S. (2016, Mar 23). Ransomware wreaking havoc in American and Canadian hospitals. *Newsweek*. Retrieved from http://www.newsweek.com/ransomware-wreaking-havoc-american-and-canadian-hospitals-439714

Lipton, E., Sanger, D.E., & Shane, S., (2016, Dec 13). The perfect weapon: how Russian cyberpower invaded the U.S.. *The New York Times*. Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=rank&module=package&version=highlights&contentPlacement=1&pgtype=collection&_r=0

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C.S. (2016). Cyber threats to health information systems: a systemic review. *Technol Health Care*, 24, 1-9.

Marx, D.A. & Slonim, A.D. (2003). Assessing patient safety risk before the injury occurs: an introduction to sociotechnical probabilistic risk modelling in health care. *Qual Saf Health Care*, 12(Supp II), ii33-38.

McCoy, T.H. Jr., Perlis, R.H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010-2017. *JAMA,* 320(12), 1282-1284.

Medicare and Medicaid Programs; Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers, 81 Fed. Reg. 63860 (Sept 16, 2016) (to be codified at 42 C.F.R. 403, 416, 418, 441, 460, 482, 483, 484, 485, 486, 491, & 494).

Morton, A.P. (2011). Hospital safety and complexity. *British Medical Journal,* 342, 514.

Nakashima, E. (2018, Jan 12) Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.d3c66123570b

Naylor, B. (2018, Mar 23). Russia hacked the U.S. power grid- so what will the Trump administration do about it?. *NPR*. Retrieved from https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it

Office of the Assistant Secretary for Preparedness and Response. (2017 Apr 27). Office of the Assistant Secretary for Preparedness and Response, ASPR Organization. Retrieved from https://www.phe.gov/about/aspr/pages/default.aspx

Office of the Assistant Secretary for Preparedness and Response. (2015 June 2). Emergency support functions. Retrieved from https://www.phe.gov/Preparedness/support/esf8/Pages/default.aspx#8

Perakslis, E.D. (2014). Cybersecurity in healthcare. *N Engl J Med*, 371 (5), 395-397.

Perlroth, N. & Sanger, D.E. (2018, Mar 15). Cyberattacks put Russian fingers on the switch at power plants, U.S. says. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html

Perlroth, N. & Sanger, D.E. (2017, May 12). Hackers hits dozens of countries exploiting stolen N.S.A. tool. *The New York Times*. Retrieved from https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?_r=0

Radke, B.A., Waters, M.J., Cleary, J.C., Evans, D., & Kittle, C. (2016, July 18). Ransomware rises among hospitals. Lexology. Retrieved from http://www.lexology.com/library/detail.aspx?g=8f3d29a5-2f87-42b8-ada1-54a109e38b3f

Sauer, L.M., McCarthy, M.L., Knebel, A., & Brewster, P. (2009). Major influences on hospital emergency management and disaster preparedness. *Disaster Med Pub Health Prep*, 3(S1), S68-73.

Siwicki, B. (2017 Apr 18) Hackers hit 320% more healthcare providers in 2016 than in 2015, per HHS data. *Healthcare IT News*. Retrieved from https://www.healthcareitnews.com/news/hackers-hit-320-more-healthcare-providers-2016-2015-hhs-data

Squitieri, T. (2002, May 5). Cyberspace full of terror targets. *USA Today.* Retrieved from https://usatoday30.usatoday.com/tech/news/2002/05/06/cyber-terror.htm

Stohl, M. (2007), Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?. *Crime Law Soc* Change, 46, 223-238.

The Joint Commission. (2017 May 10). Hospital accreditation. Retrieved from https://www.jointcommission.org/accreditation/hospitals.aspx

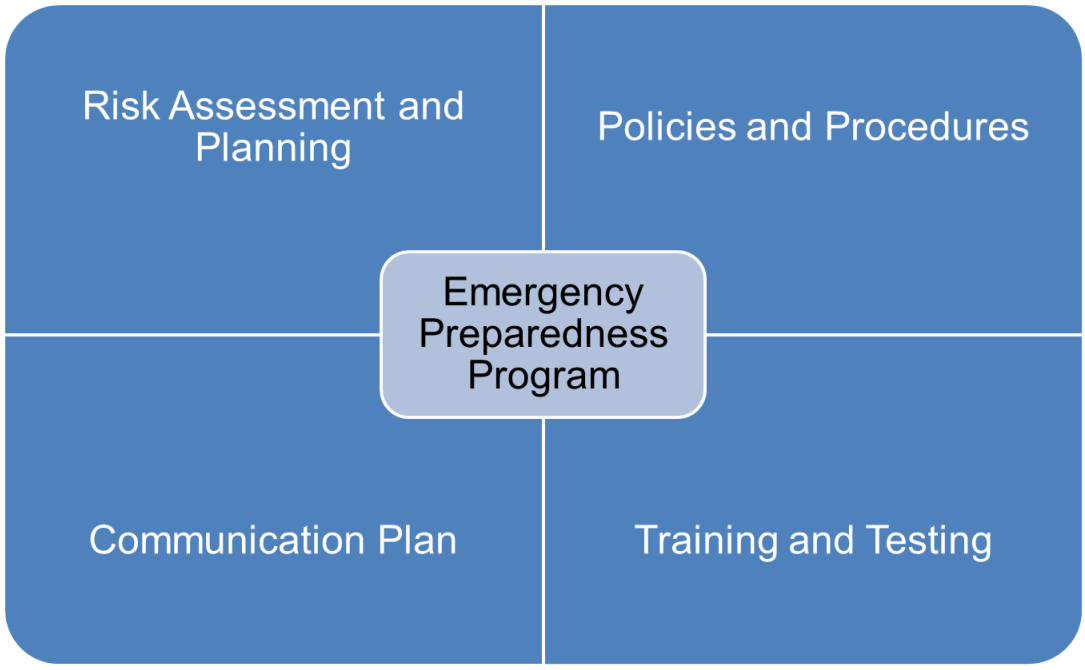
The Joint Commission E-dition. (2016, Jan 1). Hospitals: emergency management. Retrieved from https://www.jointcommission.org/standards_information/edition.aspx

The White House. (2013 Feb 12). Presidential policy directive—Critical infrastructure security and resilience. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Weimann, G. (2005). Cyberterrorism: the sum of all fears?. *Stud Conflict Terrorism*, 28, 129-149.

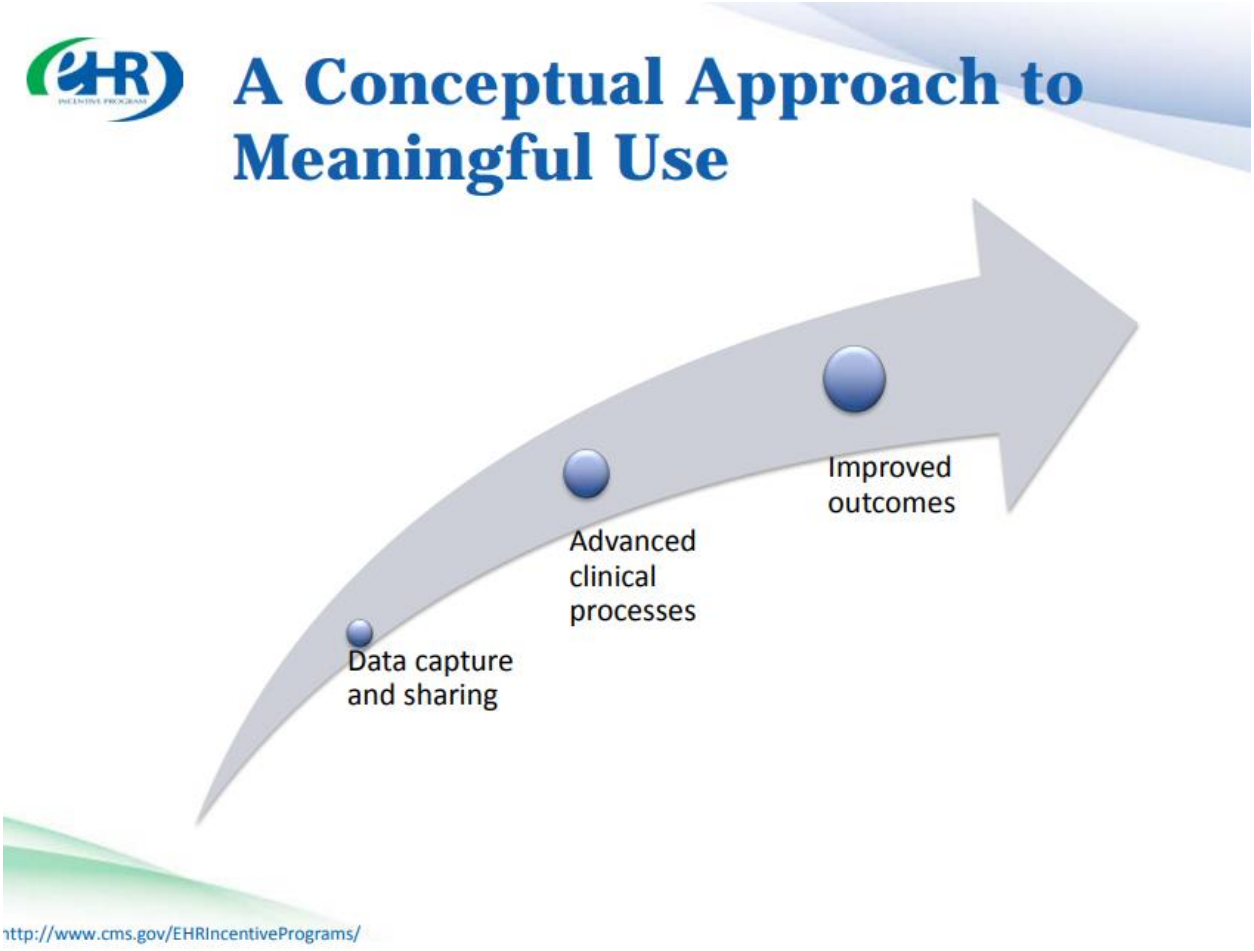
Zetter, K. (2016, Mar 30). Why hospitals are the perfect targets for ransomware. *Wired*. Retrieved from https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

Figure 1: CMS emergency preparedness requirements for qualified providers



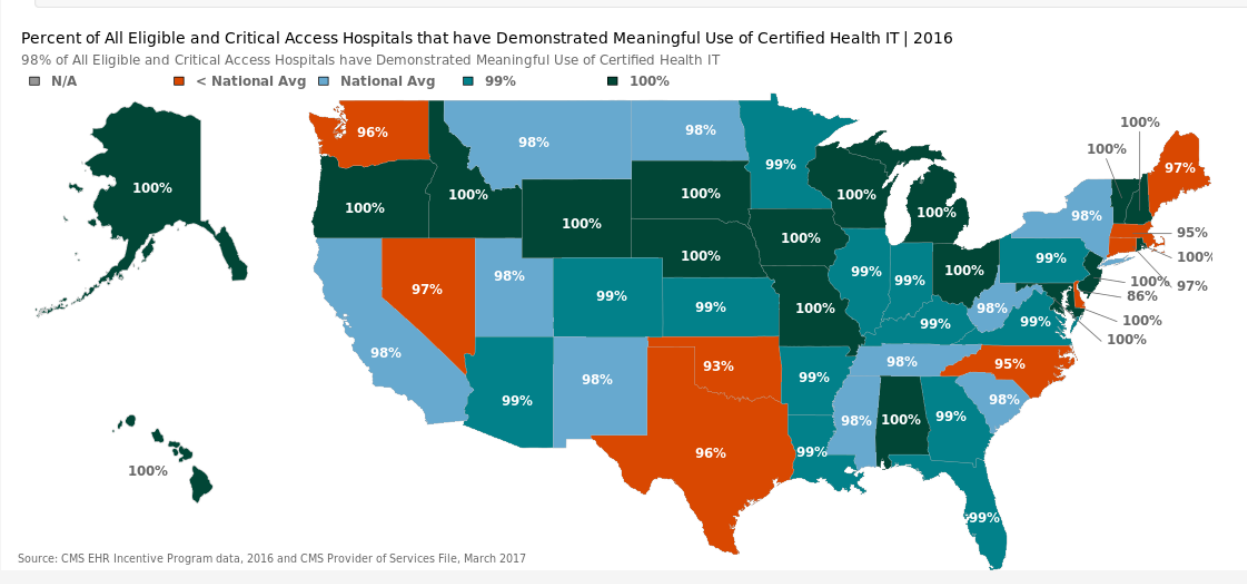
Source: Centers for Medicare and Medicaid Services. (2018). Emergency Preparedness Rule. Retrieved from https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html

Figure 2: CMS Electronic Health Record Incentive Program



Source: Centers for Medicare and Medicaid Services. (2010). Medicare & Medicaid EHR Incentive Program: Meaningful use stage 1 requirements overview. Retrieved from https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/MU_Stage1_ReqOverview.pdf

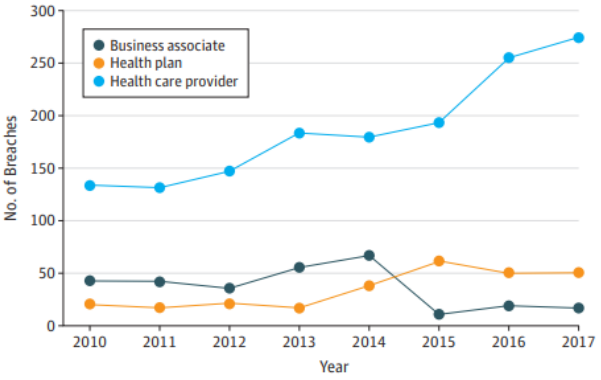
Figure 3: United States hospitals using certified health IT, 2016



Source: Office of the National Coordinator for Health Information Technology. 'Hospitals Participating in the CMS EHR Incentive Programs,' Health IT Quick-Stat #45. dashboard.healthit.gov/quickstats/pages/FIG-Hospitals-EHR-Incentive-Programs.php. August 2017

Figure 4: Health Breach Summary, 2010-2017

Figure 1. Annual Breach Volume by HIPAA Entity Type



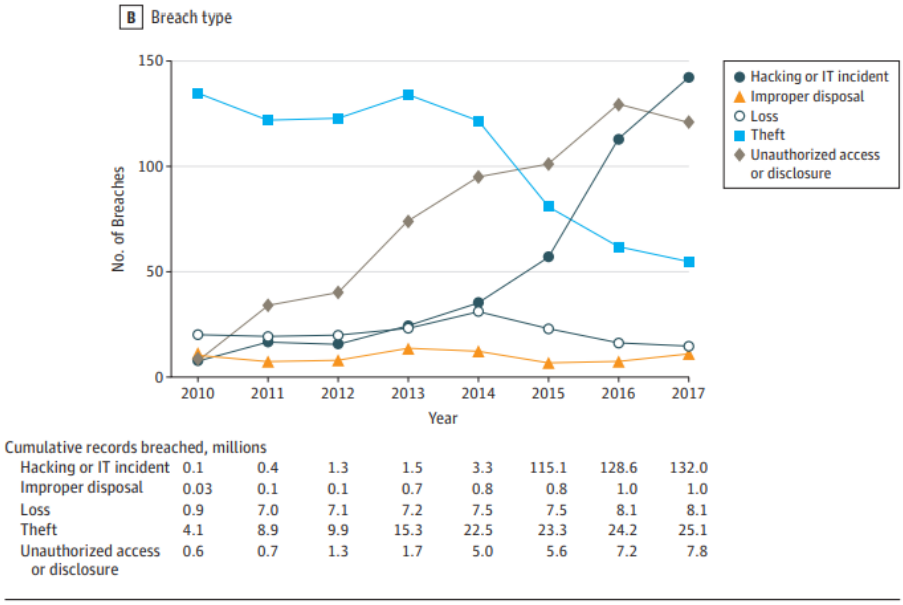
Cumulative records breached, millions

Business associate	1.5	10.5	11.6	12.6	21.0	25.0	28.5	28.7
Health plan	3.6	3.7	4.0	4.1	6.2	109.1	110.0	110.4
Health care provider	0.8	5.0	6.3	12.1	14.1	20.5	32.7	37.2

The numbers below each year refer to cumulative number of records breached up to that year. *Business associate* refers to entities that do not provide or reimburse health care but are given access to Health Insurance Portability and Accountability Act (HIPAA)–protected data, generally to support physicians or health plans. Broadly speaking, a *health care provider* is a person or organization who furnishes, bills, or is paid for health care service; a *health plan* provides, or pays the cost of, medical care (US Code of Federal Regulations 160.103). The 4 breaches of a health care clearing house were omitted for clarity.

Source: McCoy, T.H. Jr., Perlis, R.H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010-2017. *JAMA,* 320(12), 1282-1284.

Figure 5: Health breach data by breach type, 2010-2017



Cumulative records breached, millions

Hacking or IT incident	0.1	0.4	1.3	1.5	3.3	115.1	128.6	132.0
Improper disposal	0.03	0.1	0.1	0.7	0.8	0.8	1.0	1.0
Loss	0.9	7.0	7.1	7.2	7.5	7.5	8.1	8.1
Theft	4.1	8.9	9.9	15.3	22.5	23.3	24.2	25.1
Unauthorized access or disclosure	0.6	0.7	1.3	1.7	5.0	5.6	7.2	7.8

As breaches were assigned to multiple categories, totals in panels A and B exceed those reported in Figure 1. The numbers of cumulative records placed below each year refer to cumulative number of records breached up to that year. All categories were as reported in the federal database. Plots omit "unknown," "other," and "other portable electronic device" categories, determined a priori to be too open-ended to imply particular action. IT indicates information technology.

Source: McCoy, T.H. Jr., Perlis, R.H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010-2017. *JAMA,* 320(12), 1282-1284.

II. Chapter 2

Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017

Authors:
Lauren E. Branch[1]
Warren S. Eller[2]
Tom K. Bias[3]
Michael A. McCawley[1]
Douglas J. Myers[1]
Brian J. Gerber[4]
John R. Bassler[5]

Affiliations:
[1]Department of Occupational & Environmental Health Sciences, West Virginia University, Morgantown, WV 26506, USA
[2]Department of Public Management, The City University of New York, New York, NY 10019, USA
[3]Department of Health Policy, Leadership & Management, West Virginia University, Morgantown, WV 26506, USA
[4]School of Public Affairs, Arizona State University, Phoenix, AZ 85004, USA
[5]Department of Biostatistics, University of Alabama at Birmingham, Birmingham, AL, USA

Abstract

Introduction: The healthcare industry has begun seeing a new hazard develop against them- the threat of cyberattack. Beginning in 2016, healthcare organizations in the United States have been targeted for malware attacks, a specific type of cyberattack. During malware incidents hackers can lock users out of their own network to gain access to information or to hold the organization for ransom. With the increase in medical technology and the need for access to this information to provide critical care, this type of incident has the potential to put patient lives and safety at risk.

Methods: A content analysis was conducted to assess the trend of attacks on healthcare organizations. U.S. Healthcare IT News and Becker's Hospital Review were used to collect all publicly reported malware attacks against U.S. healthcare organizations between 2016 and 2017. A logic diagram was also developed to illustrate how hackers gain access to a healthcare network using malware.

Results: There were 49 cases of malware attacks against U.S. HCOs identified. The attacks occurred across 27 states, and they took place during 18 out of 24 months. Six of the organizations reported paying ransom, whereas 43 organizations did not pay or did not report payment to the press. Impacts of these attacks range from network downtime to patient and staff records being breached.

Discussion: Malware attacks have the potential to impact care delivery as well as the healthcare facility itself. Even though this study identified 49 malware attacks, we know this number is significantly higher based on data from HIMSS and the FBI. A reporting loophole exists in that hospitals are only required to report attacks in the case of breached protected health or financial data. For HCOs to fully understand the risk cyber threats pose, it is important for attacks to become public information and for lessons learned to be shared. Future research reviewing identified attacks could help identify best practices for the healthcare industry to better prepare for cyberattacks.

Introduction

Recently the healthcare industry has been facing a new type of hazard; bad actors have started targeting hospitals and other healthcare facilities for cyberattacks. This industry is particularly vulnerable to cyberattacks because healthcare providers depend on up to date information from electronic health data. This information includes patient histories and test results which is often needed at a moment's notice to provide critical patient care. Approximately 95% of hospitals in the United States use health information technology, such as electronic medical records (Luna, Rhine, Myhra, Sullivan, & Kruse, 2016). Many other health technologies including glucose meters, IV pumps, and implanted medical devices are also connected to and dependent on the hospital's network. With patient safety on the line, hospitals may be more willing to pay for restored access to their network. Healthcare organizations (HCOs) have become much more reliant on health information technology over the past decade. Another vulnerability that makes hospitals susceptible to cyberattacks are the out of date cybersecurity systems at many facilities and limited training for staff on safe cyber practices (Kruse, Frederick, Jacobson, & Monticone, 2017). These characteristics combined make HCOs good targets for attack (Luna et al., 2016; Waddell, 2016).

The cyber threats HCOs now face are complex and can come both internally and externally to the network (Narayana Samy, Ahmad, & Ismail, 2010). In a survey conducted by the Healthcare Information and Management Systems Society (HIMSS) of healthcare organizations, 37.6% of respondents said their most recent security incident was caused by an online scam artist, whereas 20.8% reported a negligent insider and 20.1% reported a hacker as the cause (HIMSS North America, 2018). There are also many points of entry in to a healthcare network which have the potential to make them extremely vulnerable (See Figures 1 and 2). A point of entry is a way for bad actors to gain access to a hospital computer or network in order to achieve something malicious, whether that be stealing data or delivering a payload virus

(Ayala, 2016). Some points of entry identified in the HIMSS Cybersecurity Survey include email, infected hardware or software, compromised medical devices, third party website, and a provider or a service linked to the network via the cloud (HIMSS North America, 2018). Some additional points of entry include internet access, a wireless network, removable media (i.e. USB drive, laptop), or theft of equipment (Ayala, 2016). Another way hackers attack is through backdoors or unpatched vulnerabilities, which are essentially access points left open across the network.

Figure 1 displays a sample hardware network of an HCO. Each switch on the diagram represents multiple devices connected to the network, and each device presents their own multiple points of entry via e-mail, the internet, or USB connections. Once an infected phone is connected to a computer or an infected link from an email is clicked, a virus can be transferred to the network and spread. Figure 2 shows an example of a software network within an HCO. In this example, there is a virtual interface with a corporate office with its own clinical and administrative management software. There are also interfaces with many different applications used around the organization, including imaging, labs, pharmacy, payroll, and patient scheduling. Each of the applications represents potential points of entry for bad actors to break in to the organization. HCOs must rely on their corporate interfaces as well as third party vendors to keep their products secure with up-to-date protections. With so many different points of entry in to the HCO hardware network, these networks have become extremely intricate and therefore highly susceptible to unauthorized access. This complexity also serves to make the network's hard to secure.

Hackers use different attack techniques to take advantage of HCO vulnerabilities and gain access to the network. A common type of attack is a phishing scam conducted over email. Hackers send an authentic looking email to hospital staff and include a link or attachment that unsuspecting users open or click. Once that content is activated, the hacker gains access to

the network and can get information or activate a malicious virus (Ayala, 2016). Phishing scams are on the rise; there was a 789% increase in phishing e-mails from the last quarter in 2015 to the first quarter in 2016 (Becker's Hospital Review, 2016 Jun). A second type of attack is a malware attack, which is when malicious code or virus is dispatched within a computer network (Narayana Samy et al., 2010). One example of malware attack that is of growing concern for healthcare organizations is ransomware. In the HIMSS 2018 Cybersecurity Survey, respondents ranked perceived threats and ransomware is now second on the list (11.3%), whereas natural hazard (i.e. fire or flood) was eleventh on the list (8.3%) (HIMSS North America, 2018).

During a ransomware attack, bad actors will lock users out of a network and demand a ransom payment for the decryption key. The first ransomware attack took place in 1989 when an AIDS researcher, Joseph Popp, sent 20,000 floppy disks to AIDS researchers in 90 countries. The floppy disks were said to contain a questionnaire to help determine patient's risk of contracting AIDS. When inserted, these disks infected the computer with a virus that lay dormant until the 90th time they were turned on. Once the computer was booted for the 90th time, a note would appear on the screen asking for licensing fees to be paid while locking the user out of the computer (Waddell, 2016). Since 1989, ransomware attacks have continued and are now categorized as one of two types: scareware and crypto ransomware. Scareware will inform a computer user there is something fatally wrong with their machine and offer a solution for a small payment. Crypto ransomware is much more complex, in that it will encrypt computer files so that they need a certain decryption key to be opened. These crypto-viruses have become a lot harder, and many times impossible, to break even by experts (Waddell, 2016).

Similar to the first ransomware attack, hackers have again shifted their targets to the healthcare industry. In healthcare, this type of attack can essentially shut down an organization's ability to operate and provide patient care (Siwicki, 2017b). In May 2017, a global

ransomware attack known as WannaCry was perpetrated by the North Korean government (Nakashima, 2018). Hackers utilized a stolen National Security Agency (NSA) tool to gain access to 300,000 computers across 150 countries (Chappell & Neuman, 2017; Nakashima, 2018). During this attack, 36 health organizations, including hospitals, ambulance services, and physicians' offices, in Great Britain were locked out of their systems (Perlroth & Sanger, 2017). WannaCry forced the National Health Service to send patients away from certain facilities in order to receive the care they needed (Perlroth & Sanger, 2017). Homeland Security experts have said this attack directly put patients' lives at risk (Chappell & Neuman, 2017).

This type of cyberattack against organizations has become more frequent in occurrence (Larson, 2017). In April 2016, there was a 159% jump seen in ransomware attacks from the month before. This was a huge rise from the normal 9-20% monthly increase that had previously been seen (Lee, May 2016). In 2015, across all industries, the Federal Bureau of Investigation (FBI) reportedly received more than 2,500 ransomware complaints, which cost the victims $214 million (Radke, Waters, Cleary, Evans, & Kittle, 2016). A 2016 IT report stated 93% of phishing emails now contained ransomware (Becker's Hospital Review, 2016 Jun). In 2018, the city of Atlanta fell victim to a ransomware attack and lost many of its critical municipal systems. This attack alone cost the city $2.7 million to recover (Spitzer, 2018).

In February 2016, an outbreak of ransomware attacks against United States hospitals began at Hollywood Presbyterian Medical Center in Los Angeles, California. The hospital was offline for over a week before deciding to pay the ransom (Barrett, 2016). Approximately $17,000 was paid and the hospital regained access to its operating systems (Winton, 2016). Since this initial attack, there has been a surge in reported malware attacks of healthcare providers across the United States. These attacks can be extremely costly for HCOs (Reed, 2016). A hospital in New York was attacked in 2017 and it has been estimated that their recovery cost was almost $10 million, including hardware, software, extra staff hours, overtime

hours, and loss of business costs (Davis, 2017). The on-going fixes and upgrades to the hospital system are estimated to be an additional $250,000 to $450,000 a month (Davis, 2017). In the most recent HIMSS Cybersecurity Survey, 75.7% of respondents reported a significant security incident in the past 12 months (HIMSS North America, 2018).

The best way for hospitals to protect themselves is to be proactive and take steps to strengthen their potential vulnerabilities and weaknesses. Hospitals need to conduct risk assessments to better understand how large the risk malware attacks pose to their organization, as well as how big an impact successful attacks can have on operations. Once they have a risk analysis of malware attacks, HCOs can decide which fixes to their system make the most sense financially to offer the most protection.

Lack of reliable reporting on frequencies and impact of this type of attack make it difficult for the healthcare industry to better secure their systems. The risk reports that do exist do not expand on the nature and scope of these successful attacks. Some of these incidents only affect a few computer terminals, whereas other incidents have a more significant impact on the organization and have the potential to affect patient care and safety. Due to the inherent nature of hospitals and the initial ransom payment made by Hollywood Presbyterian Medical Center, these types of incidents are only expected to continue to grow in frequency.

A recent study assessed trends in data breach reports to DHHS Office for Civil Rights Portal, which included data breaches caused by hacking or IT incident (McCoy and Perlis, 2018). However, this study was unable to identify which data breaches were linked to a malware or ransomware event, and not all ransomware or malware events result in a reportable data breach. Currently, there are popular media reports on these types of attacks, but there is no methodology for consistently tracking hospital attacks over time. This study seeks to address this gap by assessing the trend of malware attacks on HCOs over time. This objective

will be achieved by reviewing publicly-reported, successful attacks on healthcare organizations within the United States between 2016 and 2017. The final product of this analysis will be a timeline of reported ransomware attacks on hospitals, as well as a summary of what data is being reported with each attack. A logic diagram will also be developed to show the process of a malware attack on an HCO. Without a better understanding of this type of threat, healthcare organizations cannot adequately protect their organization or their patient's safety (Narayana Samy et al., 2010).

Methods

A content analysis was conducted of news articles related to hospital malware attacks. The new sites Healthcare IT News and Becker's Hospital Review were used as data sources. Healthcare IT News is a site published by Healthcare Information and Management Systems Society (HIMSS), and is one of the most comprehensive news sources for information on healthcare information technology. Becker's Hospital Review is another well-known and reputable source of information related to information technology in the field of healthcare. A search of these databases was conducted using a combination of the keywords "hospital" or "healthcare", "malware" or "ransomware" and "attack". These articles were reviewed for relevance to the research question. Inclusion criteria for articles were references to malware or ransomware attacks on hospitals or healthcare facilities within the United States during 2016 and 2017. Articles that discussed data breaches caused by hackers or misplaced hardware, as well as articles that discussed phishing scams were excluded from this analysis.

The included articles were analyzed to identify cases, which were then were formatted into timelines to summarize the number and locations of reported malware attacks. Upon further investigation and research, each case was also reviewed for date of attack, name of facility or organization, location, how many facilities were affected, what the impact on the

facility was, and if any outcome was disclosed. If the articles referenced a data breach, that information was cross referenced with the U.S. Department of Health and Human Services Office of Civil Rights Breach Report Database. The HITECH Act requires that all data breaches impacting 500 or more individuals be reported in this database. This data was put in to a table to summarize the extent of publicly-reported malware attacks on United States hospitals between 2016 and 2017, and to identify trends within this dataset.

A logic diagram was also created to illustrate a malware attack on a hospital network through a phishing attempt. This diagram walks through the steps of a phishing ransomware attack in which a hacker gains access to the network. The diagram was created using data collected during qualitative interviews with subject matter experts, including a Chief Information Officer, a Chief Information Security Officer, a Senior Network Administrator, and a Healthcare IT Manager. It uses a hypothetical hospital to show the extent of a successful phishing attack, and the breadth of access to data and applications a hacker could potentially gain in to a secure network.

Results

Malware Attacks, United States 2016-2017

Overall this study discovered 49 reported cases of malware attacks on U.S. Healthcare Organizations during 2016 and 2017. Within the found instances, there were 22 malware attacks in 2016 and 27 malware attacks in 2017. Figures 3 and 4 present these healthcare attack cases, respectively. This analysis has shown attacks occur all over the country and take place all year long. The data collected showed there were malware attacks on HCOs in 13 states in 2016 and 20 states in 2017. A map of the United States displaying frequency of malware attacks for both years is shown in Figure 5. The state with the most attacks in this content analysis was California with 9 attacks across both years. There were 10 additional

states that reported more than one attack and 16 states that experienced at least one attack across both years. Both years had attacks reported in 9 different months. The identified attacks are affecting more than just hospitals across the country. One attack against a health system impacted 10 hospitals and 250 outpatient clinics in the D.C./Maryland region. Another attack against a health system saw impacted hospitals across state lines. Some of the attacks only impacted one facility, but often that facility lost access to its medical record.

Each of the 49 identified cases did not have the same impact to their respective healthcare organization. Tables 1 through 4 present impact details of the identified malware attacks. Forty-one of the cases were labeled as 'ransomware' attacks (shown in Table 1). The articles reported that at least six organizations paid ransom (shown in Table 2). In one case (Kansas Heart Hospital), the hospital paid ransom and the hackers released only a portion of their files before demanding a second ransom. They did not pay the second ransom demand (Siwicki, 2016). The other 43 cases did not disclose a payment to the press. Some of the articles reported outage times for the organizations, which ranged from 1 day to about 2 weeks (show in Table 3). The most frequent time offline that was reported was one week. The first ransomware attack against a hospital, Hollywood Presbyterian, paid $17,000 after a stand-off with hackers and almost two weeks offline. Another major impact identified was compromised patient or staff records. Sixteen of the attacks reported no records breached. Seventeen of the attacks reported less than 50,000 records impacted. The highest number of records reported 500,000 breached records, with three other attacks reporting more than 200,000 breached records (shown in Table 4).

One of the issues identified while completing this content analysis was the lack of consistency in reporting and defining this type of attack. Across all identified cases, there were different search terms required to identify certain cases. Table 5 shows the different terms that were required to find different cases. Ten of the cases only showed up in searches using the

term “cyberattack”, eight only showed up using the term “malware”, and ten only showed up using the term “ransomware”. The other 21 cases were identified using more than one of the listed search terms. This lack in consistent reference words make it difficult to fully identify all reported cases.

Logic Diagram

Due to the complexity of healthcare organizations, there are a few steps hackers must go through to gain access. Figure 6 presents the steps as they would occur in an email phishing attack. The attack begins when a hacker sends mass emails to employees within an organization attempting to get one employee to be deceived. The email would either contain a malicious link or attachment within that would allow the hacker to gain shell credentials to the organization. With these shell credentials, depending upon the level of access they have, the hacker can gain direct access to network applications or they can find another user credential who does have access.

Once the hacker gains administrative or domain level access, they can permeate across the organization’s network to find the information they are looking for. In this scenario, Figure 6 shows the applications and confidential data the hacker would gain access to in this HCO. The software applications include: timekeeping, imaging, medical scribing, catheter laboratory services, obstetrics and gynecology clinical services, the network email exchange and all organizational file shares. From this access, the hacker has access to protected health information, proprietary business data, payroll information, and other confidential data, such as social security numbers of patients and staff members.

If the hacker’s goal is to deliver a malicious payload, such as ransomware, the hacker can choose where to drop it once they gain access to the active directory enabled applications.

They can choose a location which would cause the biggest service disruption to increase likelihood the organization will pay the ransom demand.

Once a hacker gains access to the HCO's network, the HCO itself has limited options on how to stop access. The first step is that the HCO must realize they have someone with malicious intent inside their network. Often in the case of ransomware attacks this does not happen until applications stop working or a ransom note appears on desktops across the organization. In cases like this, it is imperative the HCO shuts everything on the network down to stop the spread of the virus and to cut off the hacker's access to the network. This step would also cut off all users' access to the network and cause a complete organization-wide downtime. Once the network is shutdown, the HCO can conduct impact assessments to see how much damage has been done, if any, and can begin their recovery and business continuity processes. If the HCO decides not to shut down the network, the hacker has continued access to the network and the virus can continue to spread infecting more hard-drives.

Discussion

Over the last few years we have seen an increase in this trend of cyber targeting healthcare organizations. This content analysis found 49 instances of malware attack on U.S. healthcare organizations during the years 2016 and 2017. These attacks occurred across the county; with 27 states having a reported attack during the same period. The attacks also impact all areas of healthcare delivery, including hospitals, primary care, outpatient clinics, medical suppliers, and electronic medical record providers.

With aspects of care delivery at risk, malware attacks are a threat to patient safety (Ayala, 2016). The 49 attacks identified through this analysis had ranging levels of impact, but all were required to go offline for a period of time to stop the spread of the computer virus. Providing care without access to patient history can be hazardous. For example, without the

system's automated checks and balances in place while prescribing medications there is a chance that something in the patient chart gets overlooked. Medical devices are also at-risk during malware attacks, including therapeutic equipment (infusion pumps), life-support equipment (ventilators), and diagnostic equipment (PET scanners). Any of these devices can serve as backdoors in to healthcare networks if not secured. One report reviewed three case studies where medical devices were used by hackers to break in and move through a network (TrapX Labs, 2015).

Malware attacks can also affect patients and staff in ways other than through provision of healthcare services. Attacks can have direct impacts on the facility itself, which potentially has downstream impacts on patient care. At least one of the attacks from this analysis saw impacts to their security systems. The hospital's security cameras went offline, and they were forced to go in to lockdown until the cameras could be brought back online. Another system potentially at risk is the HVAC system. Without environmental temperature regulation, there is the possible need for evacuation of patients. Finally, as seen in other cyberattacks, the electrical grid and water treatment are also potential targets (Naylor, 2018). Without power or clean water, hospitals could no longer provide care and would also be required to move patients. Evacuation of a hospital is an extreme undertaking with regard to staffing and resource needs as well as finding equivalent bed capacity to take patients. An extreme example of the impact of power loss and evacuation on patient care was seen during Hurricane Katrina at Memorial Hospital where physicians decided which patients to save and hastened the death of others (NPR, 2013).

This is the first known content analysis to develop a list of malware attacks across the healthcare industry. One limitation of this research is the reliance on public reports of attacks. This analysis used two reputable healthcare IT databases to search for malware cases, however not all attacks are being reported. Based on reports from the FBI and HIMSS, attacks

against healthcare are occurring much more frequently than found in this analysis. The FBI urges HCOs to report attack, but ultimately this is left up to the discretion of the facility. Attacks are only required to be reported when medical or financial information has been compromised. One reason for not reporting is HCOs do not want to risk their reputation or income by being labeled a victim. This reporting loophole makes it much harder for the industry to get a clear picture of the attack trend (Evans, 2017). Another limitation is the lack of consistency in reports of each attack. This study tried to combat this inconsistency by using multiple search terms including 'malware', 'ransomware', and 'cyberattack'. With different terminology used in reports, there are potentially cases that are being reported but might not be captured by the content analysis. Even with this limitation, the dynamic understanding provided through this content analysis will illustrate the frequency and types of cyberattacks as it has not been seen before in previous research.

The sample of this analysis includes only successful attacks and no information was collected on attack attempts. There are many more institutions who are vulnerable to attack, as well as organizations that experience daily attack attempts (HIMSS North America, 2018). There is a need for the healthcare industry to push for more public data regarding this hazard. If attacks were reported to a single database, this information could be accessed in one location and used to better educate healthcare administrators on the risk cyberattacks pose to healthcare delivery and to business continuity. This information could also be used to better develop a more accurate hazard vulnerability assessment (HVA) for HCOs. A well-informed HVA is the basis for effective preparedness and response planning within emergency management.

In 2018, this trend against the healthcare industry continues to grow. As of September 2018, there have been reported malware attacks every month of the year affecting health systems, hospitals, third-party medical suppliers, hospice care, provider clinics, and medical

device manufacturers. Healthcare Organizations do have a few recommended actions they can take to protect their networks including developing a security culture within the organization. It is recommended that HCOs teach safe-use habits to all staff and test on these rules. There are also IT solutions to protect against cyberattacks, such as the use of strong firewalls, antivirus software, intrusion detection, and even limiting network access (TrapX Labs, 2015). Another avenue HCOs can explore in preparing for cyber threats is procuring cyber insurance. Costs of attacks are estimated to be in the trillions worldwide by 2020 (Siwicki, 2017a). Cyber insurance is a way to protect the HCO enterprise. Insurance companies will do a full assessment of an organization's IT capabilities and offer differing levels of coverage for a price. Often, insurance does not cover loss of revenue from downtime during attacks (Siwicki, 2017a). As this type of threat continues to evolve, so too will cyber insurance policies.

Cyber threats to our society are only expected to grow over time. A 2017 article from the American Public Health Association cited a cyber-firm report which estimates over the next five years, cyberattacks would cost the United States Healthcare system $305 billion in revenue and these attacks would affect 1 in 13 patients (Krisberg, 2017). There is a need for future research in this area to better define what happens within an HCO during an attack. Further review of attack cases could highlight lessons learned and potentially lead to identification of best practices. This research will help HCOs better understand this hazard to prepare for and plan for mitigation of this threat. The healthcare industry has a choice to make when it comes to emergency preparedness, are they going to prepare their organizations to prevent threats from becoming reality to protect patient health or are they going to rely on the recovery of cyber insurance.

References

Ayala, L. (2016). Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention. Berkely: Apress.

Barrett, B. (2016, Feb 16). Hack brief: hackers are holding an LA hospital's computers hostage. *Wired*. Retrieved from https://www.wired.com/2016/02/hack-brief-hackers-are-holding-an-la-hospitals-computers-hostage/

Becker's Hospital Review (2016 Jun 1). 93% of phishing emails contain ransomware. *Becker's Hospital Review.* Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/93-of-phishing-emails-contain-ransomware.html

Chappell, B. and Neuman, S. (2017, Dec 19). U.S. says North Korea 'directly responsible' for wannacry ransomware attack. *NPR*. Retrieved from https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

Davis, H.L. (2017, Jul 26). ECMC spent nearly $10 million recovering from massive cyberattack. *The Buffalo News*. Retrieved from https://buffalonews.com/2017/07/26/cost-ecmc-ransomware-incident-near-10-million/

Evans, M. (2017, Jun 18). Why some of the worst cyberattacks in health care go unreported. *Wall Street Journal.* Retrieved from https://www.wsj.com/articles/why-some-of-the-worst-cyberattacks-in-health-care-go-unreported-1497814241

HIMSS North America (2018). 2018 HIMSS cybersecurity survey. Retrieved from https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf

Krisberg, K. (2017). Cybersecurity: Public health increasingly facing threats. *The Nation's Health,* 107 (8), 1195.

Kruse, C.S., Frederick, B., Jacobson, T., & Monticone, D.K. (2017). Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care, 25*, 1-10.

Larson, S. (2017, May 13). Massive cyberattack targeting 99 countries causes sweeping havoc. *CNN Tech*, Retrieved from http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html

Lee, S. (2016, May 3). Ransomware attacks reached record high in April- and aren't slowing down: report. *Newsweek*. Retrieved from http://www.newsweek.com/ransomware-attacks-reached-record-high-april-and-not-slowing-down-report-455239)

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C.S. (2016). Cyber threats to health information systems: a systemic review. *Technol Health Care*, 24, 1-9.

McCoy, T.H. Jr., Perlis, R.H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010-2017. *JAMA,* 320(12), 1282-1284.

Nakashima, E. (2018, Jan 12) Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.d3c66123570b

Narayana Samy, G., Ahmad, R., & Ismail. Z. (2010). Security threats categories in healthcare information systems. *Health Informatics J*, 16 (3), 201-209.

Naylor, B. (2018, Mar 23). Russia hacked the U.S. power grid- so what will the Trump administration do about it?. *NPR*. Retrieved from https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it

NPR.(2013, Sept 10). During Katrina, 'Memorial' doctors chose who lived, who died. *NPR*. Retrieved from: https://www.npr.org/2013/09/10/220687231/during-katrina-memorial-doctors-chose-who-lived-who-died

Perlroth, N. & Sanger, D.E. (2017, May 12). Hackers hits dozens of countries exploiting stolen N.S.A. tool. *The New York Times*. Retrieved from https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?_r=0

Radke, B.A., Waters, M.J., Cleary, J.C., Evans, D., & Kittle, C. (2016, July 18). Ransomware rises among hospitals. Lexology. Retrieved from http://www.lexology.com/library/detail.aspx?g=8f3d29a5-2f87-42b8-ada1-54a109e38b3f

Reed, T. (2016, Apr 6). MedStar hackers exploited design flaw from 2007 to break into computer system. *Washington Business Journal*. Retrieved from http://www.bizjournals.com/washington/news/2016/04/06/medstar-hackers-exploited-design-flaw-from-2007-to.html

Siwicki, B. (2017, Aug 4). What to know about risk, coverage before you buy cyber insurance. *Healthcare IT News*. Retrieved from https://www.healthcareitnews.com/news/what-know-about-risk-coverage-you-buy-cyber-insurance

Siwicki, B. (2017 Apr 18). Hackers hit 320% more healthcare providers in 2016 than in 2015, per HHS data. *Healthcare IT News*. Retrieved from https://www.healthcareitnews.com/news/hackers-hit-320-more-healthcare-providers-2016-2015-hhs-data

Siwicki, B. (2016, May 23). Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money. *Healthcare IT News*. Retrieved from

http://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom

Spitzer, J. (2018, Apr 12). Atlanta's ransomware attack cost $2.7 million. *Becker's Hospital Review*. Retrieved from https://www.beckershospitalreview.com/cybersecurity/atlanta-s-ransomware-attack-cost-2-7m.html

TrapX Labs. (2015). Anatomy of an attack: MEDJACK [Medical Device Hijack]. *TrapX Security*. Retrieved from http://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf

Waddell, K. (2016, May 10). The computer virus that haunted early AIDS researchers. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/

Winton, R. (2016, Feb 18). Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. *Los Angeles Times*. Retrieved from http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Figures and Tables

Figure 1: Hardware Network Diagram

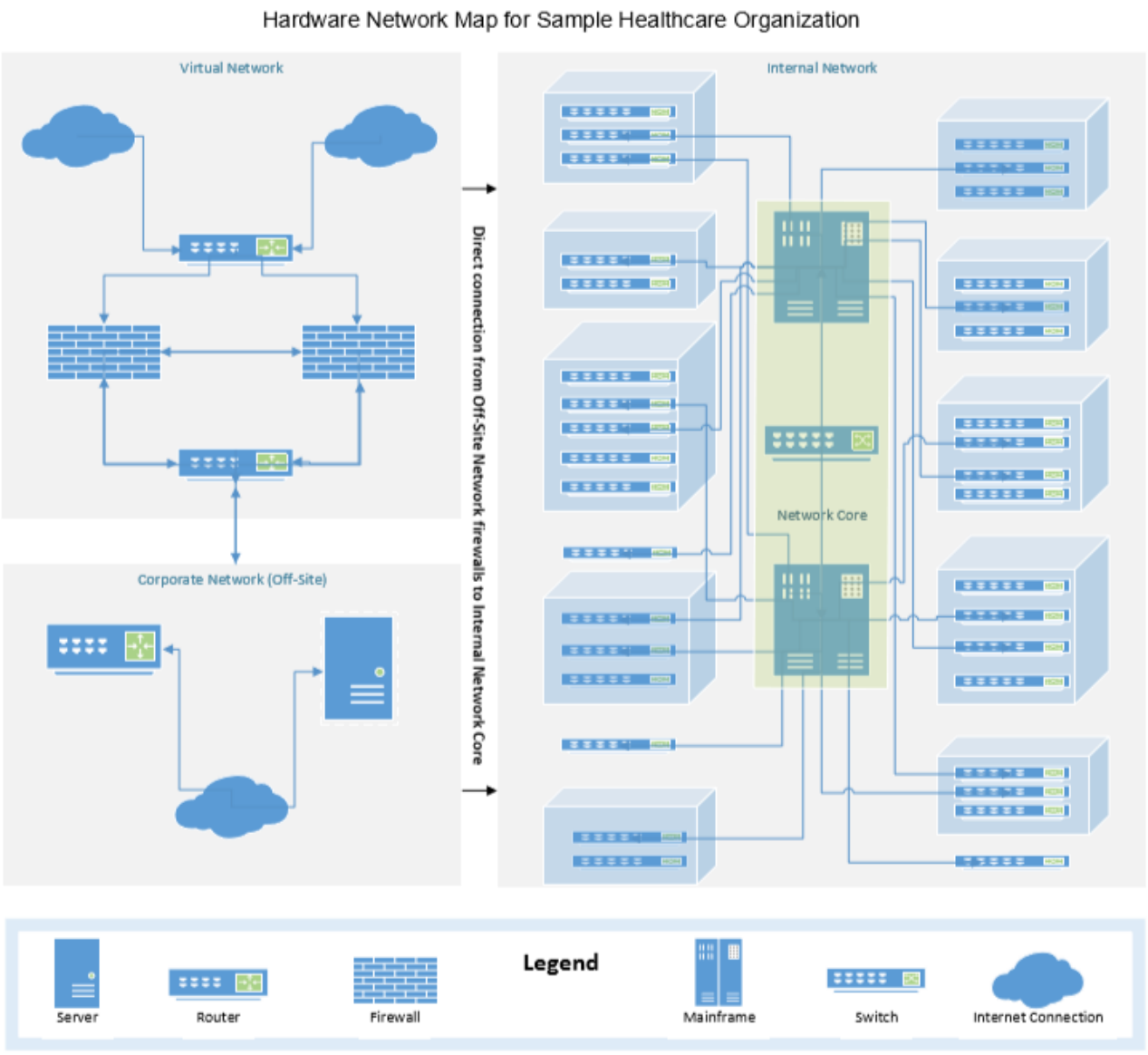


Figure 2: Software Network Diagram

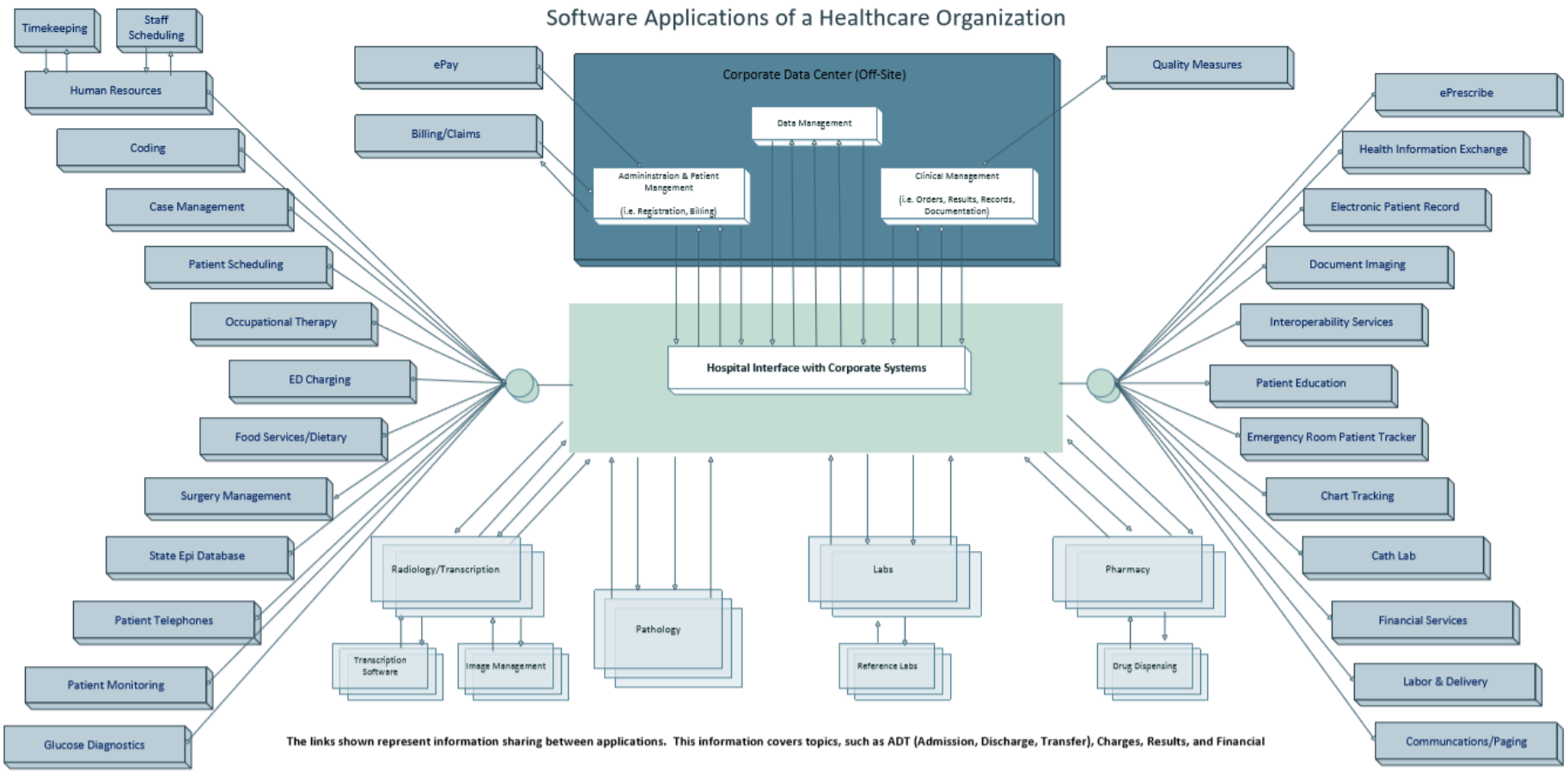


Figure 3: Timeline of Hospital Malware Attacks in the United States, 2016

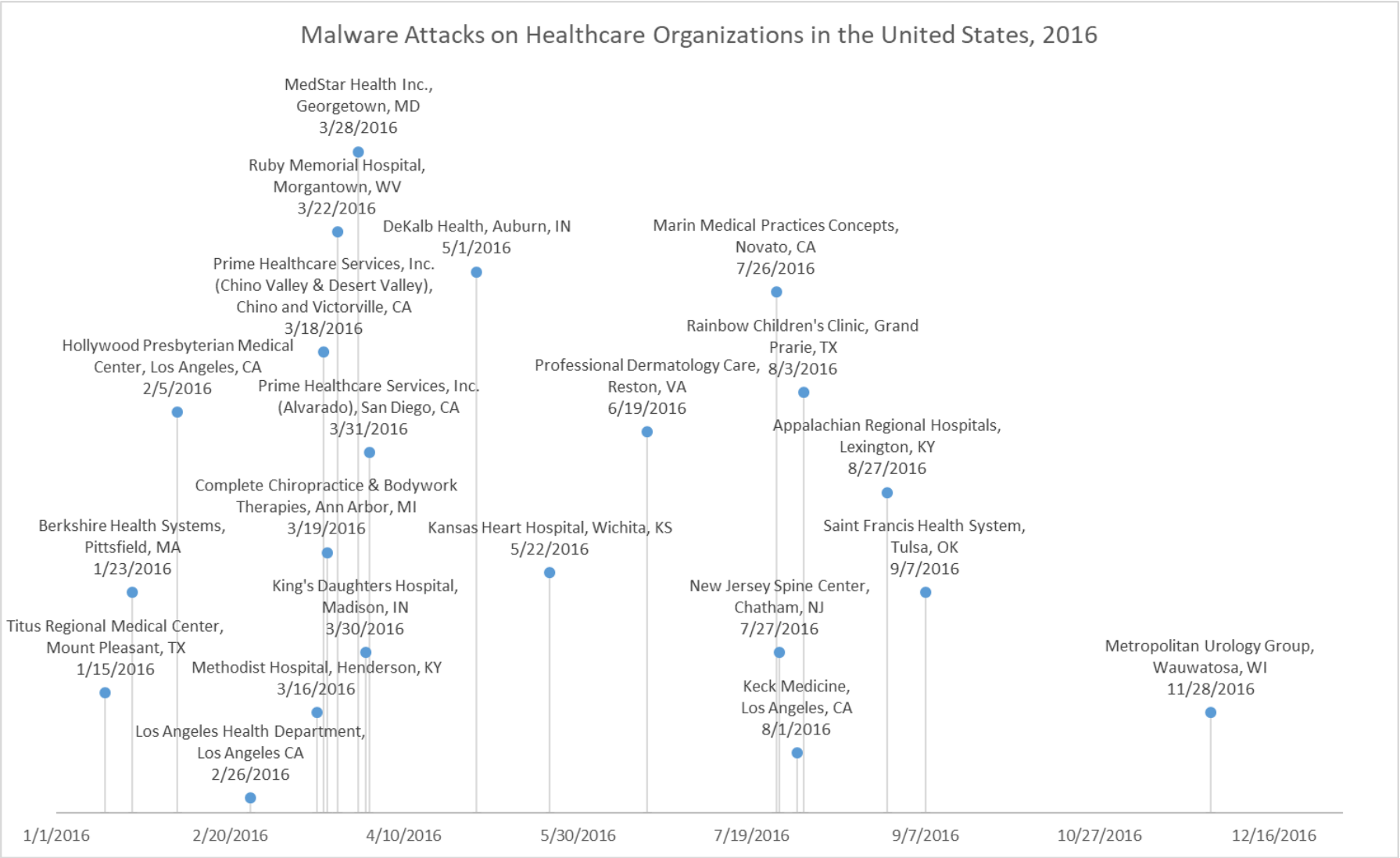


Figure 4: Timeline of Hospital Malware Attacks in the United States, 2017

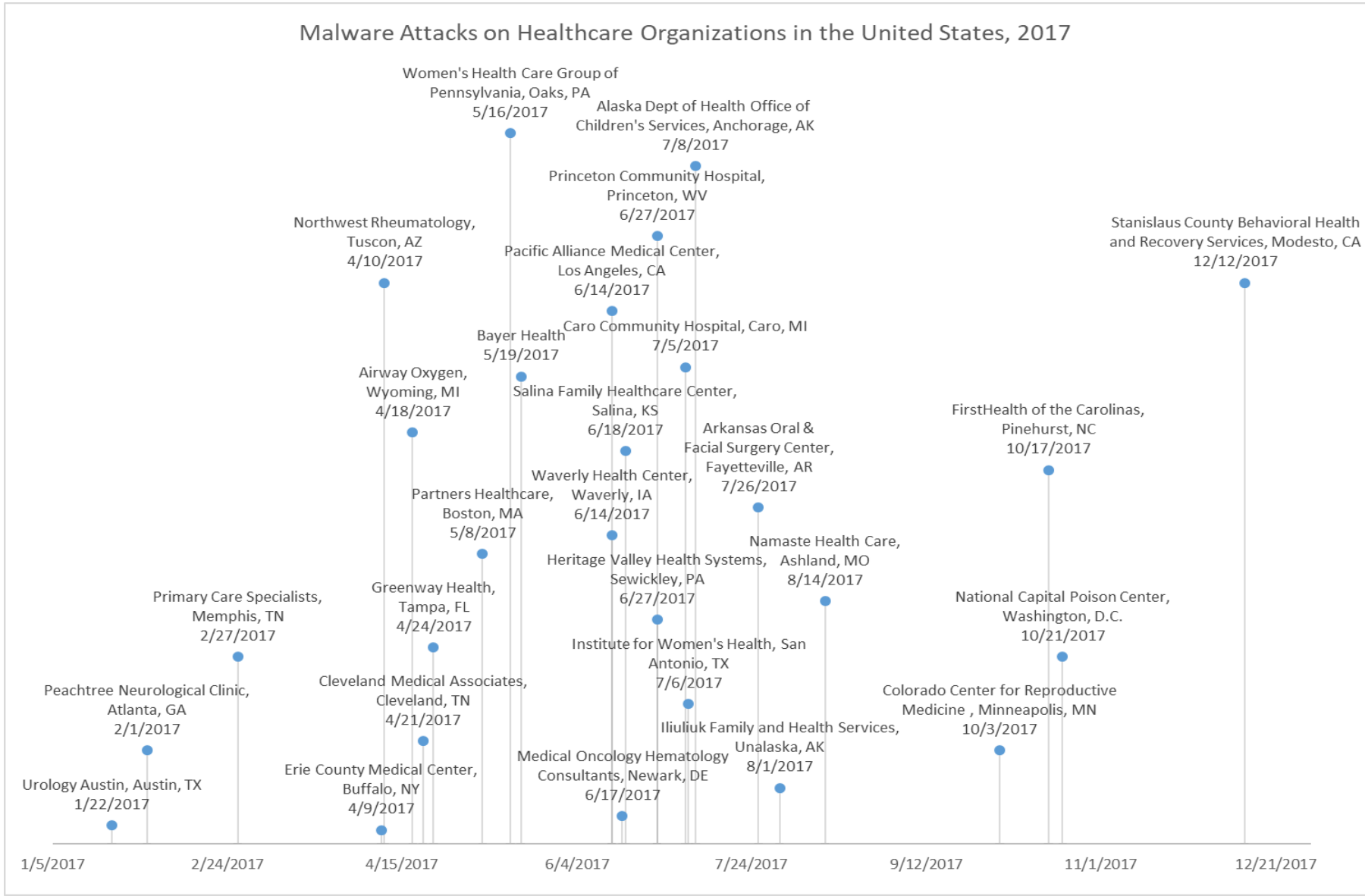


Figure 5: Frequency of Malware Attacks in the United States, 2016-2017

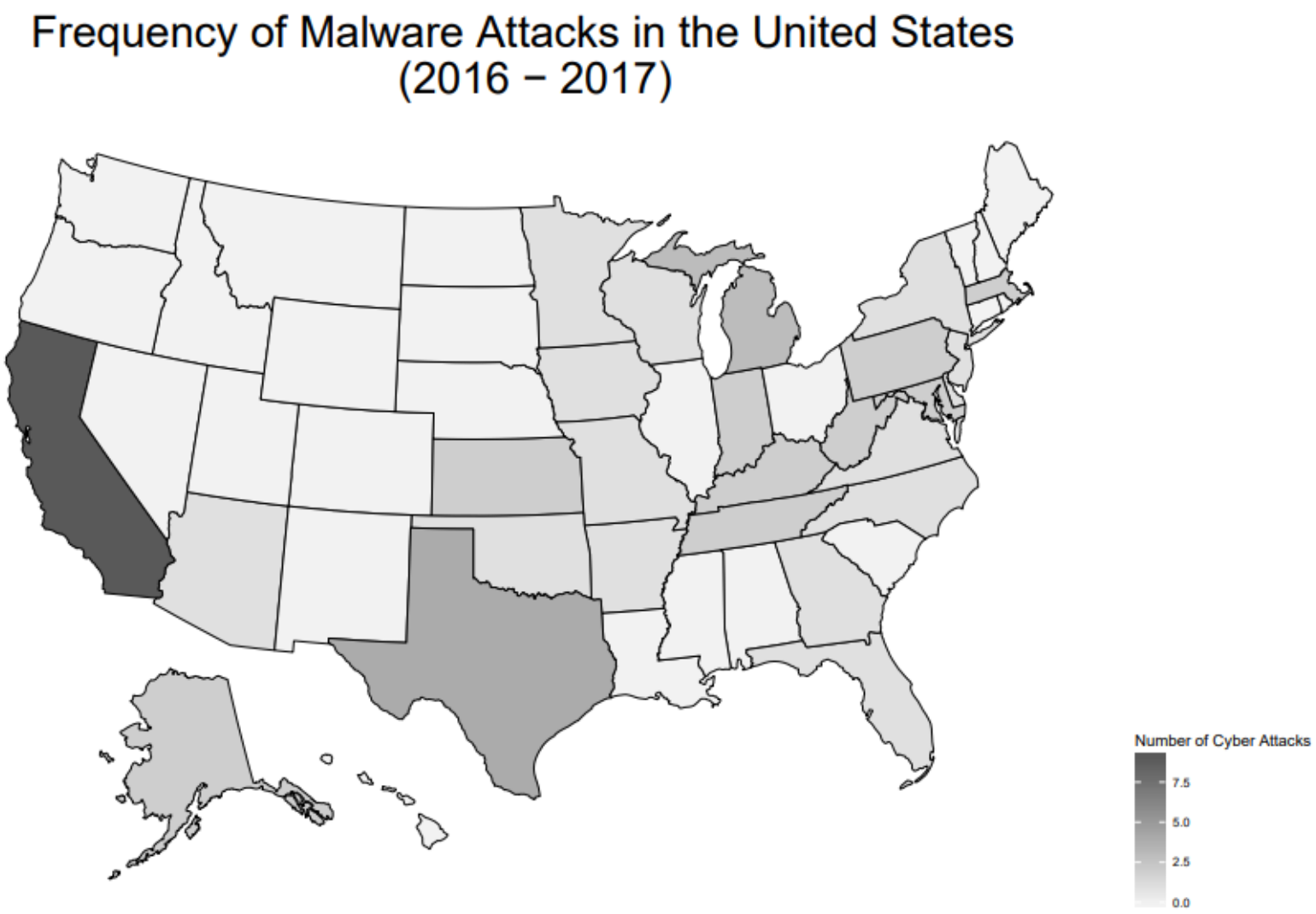


Table 1: Terminology Used to Describe Attack, U.S. Malware Attacks 2016-2017

Terminology	2016		2017		Total (N = 49)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
Malware	5	22.73	3	11.11	8	16.33
Ransomware	17	77.27	24	88.89	41	83.67

Table 2: Ransom Payments, U.S. Malware Attacks 2016-2017

Payment Reported	2016		2017		Total (N = 49)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
Yes	5	22.73	1	3.70	6	12.24
No	17	77.27	26	96.30	43	87.76

Table 3: Network/System Time Offline, U.S. Malware Attacks 2016-2017

Time Offline	2016		2017		Total (N = 14)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
1 day	0	0	2	33.33	2	14.29
>3days	0	0	1	16.67	1	7.14
>a week	3	37.5	0	0	3	21.43
1 week	1	12.5	2	33.33	3	21.43
2 weeks	1	12.5	0	0	1	7.14
> 2 weeks	0	0	1	16.67	1	7.14
3 weeks	1	12.5	0	0	1	7.14
5 days	2	25	0	0	2	14.29
Missing	14	.	21	.	35	-

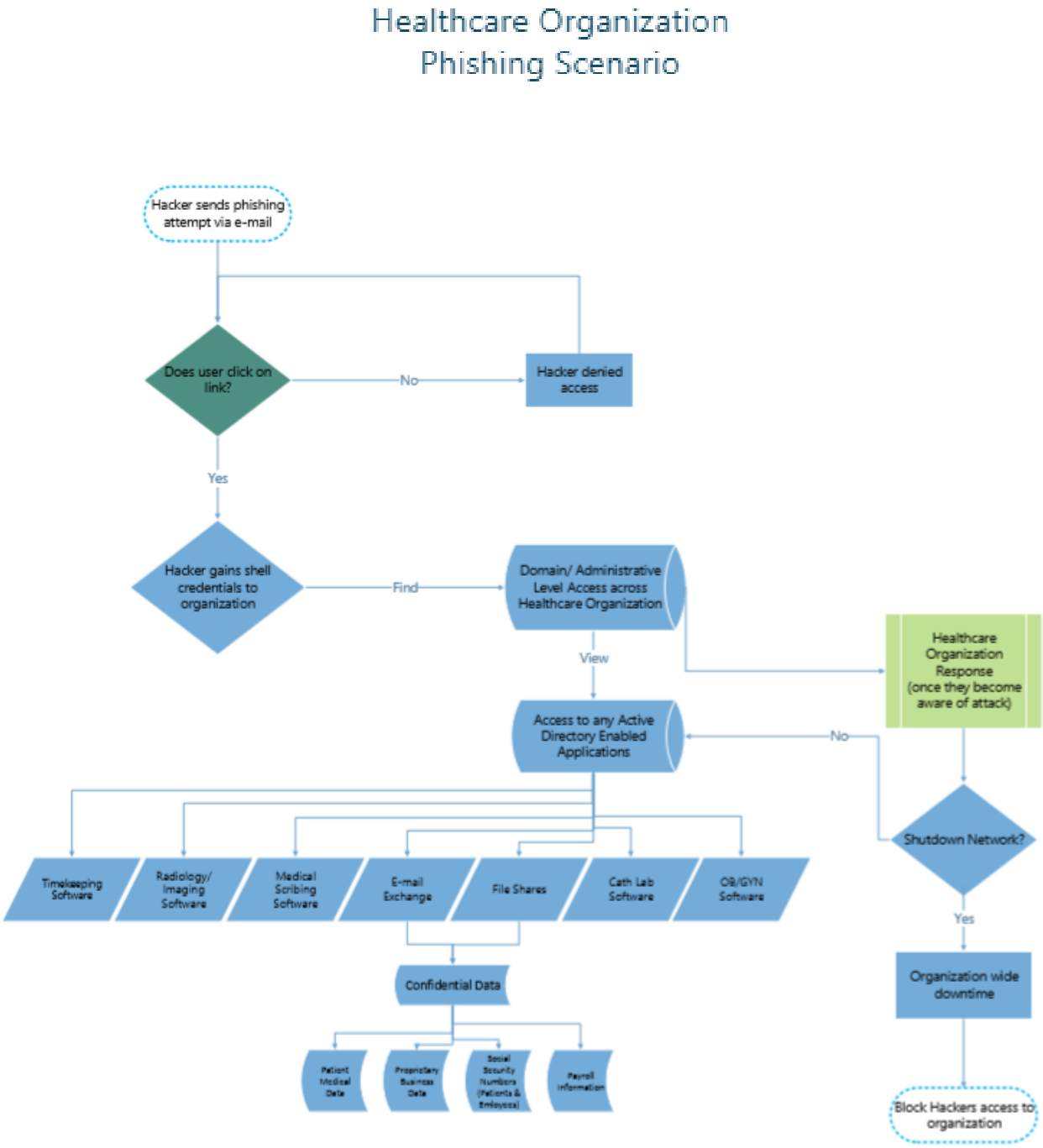
Table 4: Number of Medical Records Impacted, U.S. Malware Attacks 2016-2017

Impact Range	2016		2017		Total (N = 41)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
0	7	43.75	9	36.00	16	39.02
Less than 10,000	4	25.00	5	20.00	9	21.95
10,000 to 50,000	5	31.25	3	12.00	8	19.51
50,000 to 100,000	0	0.00	2	8.00	2	4.88
100,000 to 200,000	0	0.00	2	8.00	2	4.88
200,000 and Above	0	0.00	4	16.00	4	9.76
Missing	6	-	2	-	8	-

Table 5: Search Engine Terminology, U.S. Malware Attacks 2016-2017

Search Engine	2016		2017		Total (N = 49)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
Cyber attack	2	9.09	8	29.63	10	20.41
Malware	5	22.73	3	11.11	8	16.33
Ransomware	6	27.27	4	14.81	10	20.41
Ransomware / More than one	9	40.91	12	44.44	21	42.86

Figure 6: Logic Diagram



III. Chapter 3

Cyberattacks Against Healthcare: Stakeholders' Experiences with Organizational Response and Recovery Efforts

Authors:
Lauren E. Branch[1]
Warren S. Eller[2]
Tom K. Bias[3]
Michael A. McCawley[1]
Douglas J. Myers[1]
Brian J. Gerber[4]

Affiliations:
[1]Department of Occupational & Environmental Health Sciences, West Virginia University, Morgantown, WV 26506, USA
[2]Department of Public Management, The City University of New York, New York, NY 10019, USA
[3]Department of Health Policy, Leadership & Management, West Virginia University, Morgantown, WV 26506, USA
[4]School of Public Affairs, Arizona State University, Phoenix, AZ 85004, USA

Abstract

Introduction: Over the past three years, the healthcare industry in the United States has become a growing target for cyberattacks. This type of attack can take an entire hospital network offline and has the potential to severely impact patient safety. These cases often go unreported as the healthcare industry remains private about these incidents. Shared data on frequency and impact occurring with these attacks could be used to identify best practices for healthcare to be better prepare and respond more effectively to this type of threat.

Methods: A series of in-depth interviews were conducted with key stakeholders identified from three hospitals that have been victims of cyberattack. Each hospital was represented by an administrator, an information technology specialist, and an emergency manager. Content analysis was used to identify key themes related to cyberattacks against healthcare that emerged across multiple interviews.

Results: All of the organizations interviewed experienced complete shutdowns of their network for varied amounts of time. Two of the three organizations had to operate within incident command structure for over a month and did not fully recover for six months or more. Both organizations estimated the cost of their incident to be around $10 million. Due to the length of recovery and breadth of impact, representatives from each of the facilities felt this was the most challenging emergency they experienced during their time in healthcare. One of the key themes that emerged from the interviews was the potential risk these threats pose to patient care without digital safeguards in place to ensure accurate data. The bottom line in corporate healthcare was discussed as a barrier to being more prepared for cyber threats. The American healthcare system has become a business where the profit margin matters and augmentations to the system must show good return on investment.

Discussion: Participants in this study shared the malware attacks they experienced were not the ordinary emergency healthcare organizations prepare for, and these attacks are only expected to increase in frequency. Investments need to be made to strengthen and secure the United States Healthcare digital environment. Organizations can educate staff to be more cyber-safe while accessing the system, they could invest in IT security solutions, or go as far as restructuring their network to keep critical functions walled off from the rest of the system. With patient care and private data at risk, too much is at stake to remain vulnerable.

Introduction

The first known ransomware attack on a United States hospital was in 2016 (Siwicki, 2017). Since this initial attack, the trend of targeting healthcare organizations (HCOs) for malware attacks has only grown. A recent content analysis by the authors found 49 publicly reported attacks in 2016 and 2017. Reports from authoritative organizations, such as the Health Information Management Systems Society (HIMSS) and the Federal Bureau of Investigations (FBI), claim these attacks are occurring much more frequently. In the 2018 HIMSS Cybersecurity Survey, 75.7% of respondents reported having a significant security incident in the past 12 months (HIMSS North America, 2018). One reason the publicly reported numbers are so low is because hospitals are only required to report these attacks in instances where protected data has been breached.

Cyberattacks against healthcare can have major impacts to the organization, as well as on patient care. One major concern hospitals have are their reputations and the potential for loss of business during these attacks. These incidents can cause patients to feel that they themselves or their information is not safe. Data privacy is always an important topic in the healthcare industry and cyberattacks often put privacy at risk. Healthcare Organizations are required to report a breach of data to the Department of Health and Human Services Office of Civil Rights Data Breach Portal, and this report becomes public when there are more than 500 records breached (United States Department of Health and Human Services Office for Civil Rights, 2016). One issue that exists in the current system is the health organization itself determines whether records were accessed or breached (United States Department of Health and Human Services Office for Civil Rights, 2015). With their reputation and patient privacy on the line, there is potential for organizations to make an error during the quick call to judgement on whether records were accessed. Because hospitals often keep these incidents private, the attacks aren't being properly recorded or shared across the industry. Without reports, other

HCOs aren't aware how frequently these attacks are occurring, what happens during these incidents or how hospitals are handling them.

Another concern for HCOs is the impact to patient care these attacks can often have. Cyberattacks essentially shut down access to all or to parts of an Information Technology (IT) network. At an HCO, cyberattacks can threaten patient care equipment, such as electronic medical records (EMRs), laboratory testing technology, medication dispensing machines, active medical devices (such as IV pumps), as well as facility maintenance equipment, such as security cameras or HVAC systems. Without access to these tools, today's environment of patient care changes dramatically. In the current healthcare environment, an EMR stores all patient data and is information within a record is relied upon to make care decisions, including lab results, diagnosis information, and even allergy lists. During a cyberattack, data from all of the above technologies can no longer be trusted as accurate. Each system and all of its devices must be thoroughly inspected to make sure they have not been impacted. These changes have the potential to put patient safety at risk through improper care delivery or incorrect medication dosing or even through the inability to properly regulate environmental temperatures. This potential risk to patient safety is too high for the healthcare industry to continue keeping cyberattacks private.

Previous analysis showed that not all HCOs who fall victim to cyberattack see the same effects on their organization. Some facilities reported minimal impact to a few of their systems, whereas other facilities had to rebuild their entire network costing them millions of dollars. To understand the true risk cyber threats pose to healthcare, it is important to know the full spectrum of their potential impact. A more in-depth knowledge of previous attacks can be used to illustrate what happens to organizations under attack as well as to identify best practices for hospital preparedness and response.

The primary objective of this study is to examine the organizational best practices to mitigate the effects of and to re-establish business continuity after a malware attack. Currently, recommended actions for HCOs are somewhat generic and lacking overall with how HCOs should prepare for and mitigate the impacts of an attack. This study seeks to address this gap by assessing the organizational outcomes of a malware attack on healthcare organizations. This objective will be achieved by first identifying key evaluation questions based on existing literature and conversations with subject matter experts. These questions will then be used to interview key stakeholders in healthcare cybersecurity, including representatives from healthcare IT, emergency management, and administration, to compare outcomes of three different facilities that were each victims of a malware attack.

Methods

A series of in-depth interviews was conducted with staff from three separate healthcare organizations to answer this aim's research questions. This qualitative approach was chosen to allow for a deeper understanding and help create an in-depth description of what happens within an organization during a ransomware attack (Cagliuso, 2014a; Creswell, 2007). Hospitals selected for this study had experienced a malware attack on their organization within the previous 2 years, and the interview subjects were employed at the HCO during the time of their attack.

Interviews were conducted with three representatives from each healthcare organization. Each HCO was represented by an employee from each of the following stakeholder groups: hospital administrators, hospital safety/emergency preparedness coordinators, and health IT staff. By interviewing individuals from different stakeholder groups, the data will provide a well-rounded explanation of the phenomenon in question (Cagliuso, 2014a). Hospital administrators oversee the clinical and operational aspects of the hospital, as well as serve as decision makers in the organization's response (Cagliuso, 2014a; Cagliuso, 2014b; Healthcare IT News &

HIMSS Analytics, 2016). Hospital safety/emergency preparedness coordinators ensure the organization meets the regulatory requirements for emergency preparedness. Health IT staff ensure all IT equipment within the facility runs smoothly and securely. The participants selected were key individuals in the response to their organization's cyberattack. Interview subjects will remain confidential and will only be identified by their stakeholder group.

A semi-structured interview guide was developed using background information and research questions, including data collected from previous analysis and informal conversations that have occurred with hospital representatives. The interview will consist of open-ended questions with probes to help elicit information from the interviewees. Some of the topic areas covered in these interviews are recognition of the attack, impact of the malware on their system, an overview of their recovery efforts, preparedness efforts both before and after the attack, and whether there have been other attacks on their organization. The interview guide can be found in the Appendices. The interviews were conducted over a nine month period at times convenient to the participants. Each interview was recorded and transcribed for analysis.

Once the interviews took place, the transcripts were analyzed using content analysis. The purpose of content being analysis of documents, text, or speech to see what themes emerge from the data (Krippendorff, 1989). The data was read all the way through prior to the analysis being conducted. Multiple read throughs as well as techniques such as memoing and marking were used to help identify themes across the nine interviews (Creswell, 2007). Some key descriptions of what the stakeholders experienced are included in the paper to help illustrate the emerging themes (Cagliuso, 2014b).

Results

This study explored the lived experiences of nine stakeholders in healthcare cybersecurity. Interview questions 1-4 collected demographic information, while questions 5-9

examined issue salience and situational awareness. Questions 10-19 elicited descriptions of system impact, business recovery, and organizational preparedness. The results are displayed in three sections: participant description of the attack and its impact on their organization, the identified themes across interviews, and organizational actions taken to be more prepared. Quotes from participants are included to provide individual descriptions of the experiences discussed. The mean length of time for interview was 41 minutes.

Characteristics of the healthcare organizations are summarized in Table 1. Two of the facilities interviewed are Level One Trauma Centers, and the other facility is an acute care hospital. The average bed count between all three facilities is 509 beds. The first set of questions regarded participant demographics. This data has been summarized in Table 2. Each organization was represented by two males and one female. The average years in career field was 11.4 years. Highest level of education completed ranged from an Associate's Degree to a Doctor of Medicine, with the most common level seen across participants being a Master's Degree.

Each healthcare organization experienced a malware attack between 2016 and 2017. Two of the organizations' incidents were ransomware attacks, where the hackers asked for a ransom payment to unlock their networks. Both of these hospitals reported not making the ransom payment. The other organization reported originally seeing a ransom note on their PCs which quickly disappeared, and the organization realized this was a malware attack rather than a ransomware attack. The hacker's primary goal in this organization's incident was system damage.

While discussing the details of each organization's attack, some similarities started to become apparent. One characteristic each organization identified as helping their response and mitigation was the quick recognition of the incident by information technology (IT) staff. Each

organization realized they were infected with a virus when employees called their IT desk and reported issues with accessing certain computer applications. The IT staff member at each organization realized what was occurring and shut down their network. Hospital A expressed how important it was for their IT staff to have the authority to make this call on their own. A rapid shutdown of the network can stop the lateral spread of the virus across the system and essentially 'stop the bleeding' in terms of system impact. The Emergency Manager from this facility expressed how impactful this was for their organization:

> "Our IT folks…they have the autonomy…that if they noticed something that's hanky, they don't have to pick up the phone and call somebody and get permission to lock things up and to protect us. They have the ability that the minute they see something that's weird, they can essentially lift the plastic, hit the red button and let folks know after the fact that…something's up. So…that was a saving grace for us."

Even though each organization's quick recognition and reaction to the attack, there were still different lengths of impact and business recovery. The shortest impact was Hospital C which was back to normal business in about seven or eight days. Whereas Hospital A and Hospital B had their incident command teams activated for over a month and were not back to normal operations for six months. These facilities were required to rebuild their entire networks which was extremely time consuming and costly. This rebuilding of a network entails cleaning or replacing each PC, each hard drive, and each piece of equipment on the network; meaning for most of these facilities thousands of hard drives had to be cleaned or replaced. Both Hospital A and Hospital B shared in their interviews that the network rebuild cost more than $10 million. This cost of impact includes equipment costs, increased hours by salaried employees, and business interruption costs. The length of impact between hospitals differed because of how far-reaching the virus was through their networks. Forensic investigations revealed the

attackers had been in the organizations' networks prior to the activation of the malware virus. All facilities interviewed said the virus was believed to have been in the system anywhere from a couple of hours prior to activation up to 24 hours prior to activation. Hospital A did report the hackers had been in their system the week before the attack, most likely mapping out the hospital network. Additional time in the system allows hackers to find the most detrimental location within the network to deploy the malware virus. The goal in a ransomware attack is to cripple an agency so they feel their only way out is to deliver the ransom payment.

The length of impact was defined by how far-reaching the virus was within the healthcare system, and as a result by how many applications were affected. Two of the hospitals saw complete shutdowns during their attacks. The Administrator from Hospital A said, "everything was absolutely cutoff." The Emergency Manager from Hospital B illustrated this point a bit further,

> "Every computer system in the organization was taken out with one exception of a security computer that regulated electronic door locks and electronic badge access to the actual main campus."

When questioned for more details regarding applications that went down during the attack, all interviews mentioned patient care, business, and facility management applications were impacted. Hospitals A and B lost access to their electronic medical records (EMRs). Hospital C did not have the virus infect their EMRs itself, however they had issues with supporting applications to the EMR taking it offline for a period. Each facility was forced to go back to pen and paper records for a period of time, which will be discussed more below. These records included patient charting, medication orders, laboratory results, and radiology results. Radiology was highlighted by all facilities as being a heavily impacted department, noted because of how technology reliant they are. Hospital A was forced to go back to printing films

and having a radiologist in house to read films and dictate results. All three facilities also reported seeing impacts in the Pharmacy department. Each facility was forced to fill orders by hand and had issues accessing their medication dispensing devices. Scheduling was another piece of patient care that was affected at Hospitals A and B. All schedules for patient appointments, operations, etc. are kept electronically and were not available during the attack.

One the business side of the house, there were effects seen on the revenue processes. First, billing is done electronically and when that went down Hospital A was unable to bill out or accept payments for almost two months. The Administrator said:

> "We couldn't pull any data…So revenue-wise it was a real problem. … We couldn't bill out…bills were coming in, but we couldn't see them."

Another revenue-impacting application that was affected was the timekeeping system at both Hospital A and B. Hospital A was forced to go back to paper timecards to track employee hours. Due to the attack occurring so close to pay day, they also were unsure what was owed to each of their employees. For that billing cycle, they opted to pay employees what they were paid on their previous paycheck and to reconcile these payments once the system was back up and running. Another huge impact seen at all the facilities was loss of email. As pointed out by the Administrator from Hospital B, "No email whatsoever, imagine in today's world, no email…it was devastating."

Secondary systems were also lost in the attacks. The IT representative from Hospital B explained it as,

> "It was little side things that you assume will work no matter what, suddenly were down."

At their facility, they were unable to take credit card payments in their cafeteria. They also had a tube system through their facility that wasn't functioning properly. Hospital C reported issues seen with their sterile processing for endoscopies. Other applications were impacted simply because the network was down, meaning they were operational but had no network to talk to and nowhere to deliver their data. The IT representative from Hospital A illustrated this point by saying,

> "Modalities were working but only in isolation…without the network, they're essentially deaf, dumb and blind. You had to figure out how to do everything from the device itself."

Finally, there were varying impacts seen to security systems and HVAC systems, which will be discussed more in the following section.

Themes

A few key themes emerged from the participant narratives. Below is a discussion of these themes, as well as a few key quotes from participants to help illustrate their experiences.

Theme 1: Risk, risk everywhere

One of the topics discussed in almost every interview was how common this threat has become for the healthcare industry. The administrator from Hospital B said, "this is a constant continuous threat to all healthcare organizations." The Emergency Manager from Hospital C shared how concerned he is about keeping his organization prepared against cyber threats,

> "What frightens me is the sheer volume of cyberattacks that we see on a daily basis, coming through the hospitals. That volume is alarming, and any one of those things could get out of control and cause problems. It's a constant threat.

> …my fear is that it's going to just keep occurring and the frequency and the expansiveness of it at a facility or facilities plural [will increase]."

Each facility acknowledged they've had attack attempts on their organization since their major attack. Hospital B's IT representative said, "We have attacks daily, but none of them have penetrated our defenses since then."

Representatives from all facilities also expressed concern for the ability to keep hackers out of their systems. Multiple interviewees pointed out the race that exists between IT professionals and hackers to build more secure walls and to break down the security measures, respectively. The hackers look at this as a business and are constantly working to find ways to get around security features. The threat is continuously evolving, and IT professionals must stay aware of these almost daily changes in their field to remain secured. The Administrator for Hospital C expressed his concern for this evolution,

> "It is perpetual and just because what you did was effective yesterday or even today has no bearing on whether or tomorrow. …So, we remain vulnerable."

Another major concern expressed was how little is understood or shared about cyber threats in healthcare. The stakeholders felt that having more concrete information about this threat would provide a path forward for them. The Emergency Manager of Hospital C said,

> "I don't know that there's …a true risk assessment that's been done to understand the impact [to] operations from a malware or cyberattack."

Another participant (IT from Hospital A) expressed similar thoughts below,

> "There seems to be nobody collecting or willing to communicate exactly how much damage is actually occurring out there."

The participants felt with more data, they would be better equipped to prove how large of a risk this is and provide solutions that offer good return on investment. These stakeholders are dissatisfied with existing solutions, as well as the secrecy and the privacy between healthcare organizations. Currently, they feel the best way to protect their organization is to be better than the next organization. The IT representative from Hospital A expressed his approach below,

> "I don't think there's any way you can totally prevent them, but if they find it difficult to attack you, they're going to move onto the next person. Which to me is a sad statement to the state of healthcare security in this country because my primary defense is make sure I'm stronger than the next person. And you know, that doesn't make me feel good."

If HCOs were more open about being attacked, that information could be used to more clearly define what happens during these attacks and identify best practices for preparing organizations. This shared belief was a major reason why these three organizations agreed to be part of this study.

Theme 2: Realization of how connected we are in today's healthcare delivery environment

While all participants have worked in healthcare for years, they have each seen the healthcare industry evolve from one of paper records and orders to an almost completely digital environment. Even with this knowledge of the digital world they live in, most stakeholders expressed the shock that came during the attack realizing how connected their facility was and how many processes in their field have become automated. The Administrator from Hospital C, who is also a clinician, expressed his shock at realizing how technology dependent his organization has become in the following two quotes.

> "Frankly, I don't know that outside of IT we gave it enough due prior to that until we realized how truly dependent we were on the tech functions that go on in the

> background. The example that I use when explaining it to other folks is, we were unable to appropriately wash and sterilize endoscopes because of the malware attack. You wouldn't think that you could, that somebody affecting the computer would keep you from being able to do a colonoscopy."

> "You know, if [our Electronic Medical Record] goes down, we can't check a blood sugar. … Because our glucometers are set up that they work after scanning a patient ID so that they will automatically input the value into that patient's chart. So if you can't scan the patient's ID, because [the EMR] won't receive the function, you can't check the blood sugar."

Another major realization that occurred during their attacks was how many different applications were being utilized across their organization. One of the first steps of the response was creating a list of the applications impacted and then prioritizing them on critical function. During this process in each organization, there were applications brought up that people in the command center had no idea what they were or who was using them. The Emergency Manager from Hospital A shared, "I don't think any of us realized just how many separate, different programs that we actually had." Not only was this an issue with response, but each application on the network poses additional security risk to the organization. The Administrator for Hospital A shared this was a question when reloading applications, asking whether the application was necessary and worth the additional risk. She shared that not all applications were reloaded on to the network.

One facet of security risk brought up by the IT stakeholders was healthcare's dependence on third party's security. Today's healthcare environment uses different software applications to conduct care delivery and business operations. Most of the applications discussed above come from third party vendors. Once the application is purchased, it is often

put on the hospital's network, and if that application is not up to date with security, it can serve as a potential route of entry in to the organization's entire network. One of the IT stakeholders expressed this by saying,

> "I still think there's an issue in healthcare… it's one of the few environments I can think of that it's the inside software systems, the mechanical systems and everything are managed and created by different organizations…companies that really don't look at security as our primary goal."

One of the other IT participants expressed his concern on this topic saying,

> "We need to gear up and check and make sure all these vendors making these medical devices understand the full impact of their role in preventing this."

Theme 3: What's at stake with patient safety and environment of care

A big concern in healthcare is always data privacy, and during a cyberattack that becomes a major concern. An unwanted party has accessed a private network and potentially accessed any number of private records, including patient health or employee personnel. Hospital A spent months investigating to make sure there was no Private Health Information (PHI) was breached.

One of the first questions asked during each of these cases was 'how does this impact patient care?' In each of these cases, the organizations were able to continue care for the patients on hand. One of the facilities put their Emergency Room on diversion until they were able to get a better handle of the situation. Another facility had to cancel some surgeries scheduled for that day. Also, as discussed previously most of the normal digital processes for providing care were inaccessible to providers and there had to be work arounds put in place. Without the usual system safeguards in place and the large number of younger employees who reported not knowing how to switch back to paper charts and orders, there becomes increased

chance of error with provision of care. The hospitals in this study felt they could provide safe care for most of their patients, but they were unsure whether they could rely on the patient data they had. There was a huge concern expressed by more than one facility that health data they had for each patient was potentially no longer reliable. They worried patient charts or test results were compromised and realized how detrimental that could be when making care decisions. One of the IT stakeholders expressed his thoughts on the topic,

> "Also [the importance of making sure] that the integrity of the data is solid, this is health data for patients. Doctors and physicians and clinical staff are running with this data and providing care and that data is not solid. We can be doing really serious harm to the patient."

Another issue regarding patient care that was mentioned by the facilities was the use of medical devices, such as I.V. pumps. While participants all reported no impacts seen to medical devices at their facilities, they still had concern. A few mentioned they had read articles about the potential for active medical devices to be impacted by cyberattacks, and how there is proof that medical devices have been hacked before. The reason these facilities did not see impact to their medical devices was due to the devices being off-network or due to the virus not making it to that part of their network. One of the IT participants made this comment about his facilities' I.V. pumps,

> "Yes, they are on my network. The models that I have, have not been associated with any attack, but that's not to say that that won't come today, tomorrow, next week."

Another effect seen during these attacks which can potentially impact the patient care environment are the facility management functions. The security systems and HVAC systems both saw impacts across these three organizations. Two of the facilities reported issues with

their security systems. One facility reported their badge readers going down for a short time. The other facility reported having issues with their security cameras. One of the participants said this about their security cameras,

> "There was concern that we were not able to view our security cameras. So pretty much we were blind looking out into areas… [such as] entry points and other high-risk security areas that we would normally use video cameras to monitor."

Ensuring a secure environment is essential to providing safe care, and without the ability to control access to the facility or certain areas of the facility patients and staff are potentially put at risk. Both issues were made a priority and resolved quickly.

The third facility noted the attack had an impact to their HVAC system. The organization lost the automated controls of the system and had to monitor the environment, as well as make any adjustments by hand. A representative from that facility discussed this effect below,

> "The plant operations team actually went around and manually monitored that during our time period. They would do… hourly or daily checks to make sure everything was up and running and if they needed to tweak it, they did it by hand."

If the proper temperature cannot be maintained or ventilation becomes an issue, the facility may have to consider evacuating patients. For these three facilities, with a combined average of over 400 beds each, this would not be a simple task and moving certain types of patients could cause major health complications. The other two facilities reported they did not see impacts to their HVAC systems because one system was too old to be on the network and the other was on its own network.

Theme 4: This is not a normal healthcare emergency

One thing that became very apparent throughout the interviews was these malware attacks were unlike any other emergency healthcare organizations normally face. Reasons given in support of this statement were the length of time it took to recover, as well as the extent of impact seen across each organization. One of the Administrators expressed this sentiment by saying,

> "This was by far the most far reaching and devastating event I've ever been involved with in all my years of being in healthcare."

An Emergency Manager from a different organization expressed similar sentiments saying,

> "The challenge, the one thing that took the wind out of our sails was not so much the scope of what happened but the length of what happened. We operated in incident command mode for pretty much a month….this is not the typical disaster that a hospital faces….But this magnitude and this duration is what sets this apart."

Sometimes this type of threat is compared to downtime at a healthcare facility, where a piece of the system or applications go down. This happens often at hospitals where the IT team sets up a scheduled downtime while they deploy a security patch or sometimes when something goes wrong with an application. Hospitals prepare for these downtimes by pre-establishing downtime procedures that most staff are comfortable with. This type of event though is very different than a normal hospital downtime because during cyberattacks these facilities lost access to everything. Each of the organizations interviewed expressed their assumption that they would only lose one or two things at a time, and that in hindsight they realized how unprepared they were to function without access to anything. An Administrator pointed out:

> "We had a lot of assumptions that not everything would ever go down at once."

The Emergency Manager from another organization said,

> "We were not used to losing all of it at the same time, and that's what created the issues. We have plans for the loss of [each] thing that was impacted and we have lost everything that was impacted at one time or another, but to have lost all at the same time was the challenging part."

Another issue that arose at two of the facilities based on this assumption was their downtime procedures were stored electronically. They expected to always have some working computers or printers but had ended up having none during their initial response. Luckily, they were able to find ways around this by having a few paper copies or a laptop that had been completely unconnected from the network at the time of attack.

Theme 5: Tenured staff were our heroes

An unexpected theme that emerged during the interviews was how essential tenured staff was to the organizational response and recovery from the attack. This theme was mentioned by at least one stakeholder from all three facilities. The participants explained that staff who had been in healthcare longer were able to shift back to pen and paper records much easier than newer staff. This group of individuals had experience with paper charting during their careers. In contrast, the participants mentioned the hard time that younger staff had with switching back to paper charts. The Emergency Manager from Hospital A expressed,

> "In some cases, it was kind of humorous, a lot of the newer younger clinicians, whether it's nurses, whether it's physicians, they are so acclimated to doing everything in the electronic realm."

The tenured staff were able to show the younger generations how to do things without access to the network. All the participants who mentioned this topic were thankful they had experienced staff there who had knowledge of paper charting. The IT stakeholder from Hospital B shared her experience seeing this phenom happen during their attack,

> “That's where it was really interesting where some of the employees that had worked in healthcare long before we had the electronic arena, they were able to help many of the team members who had basically grown up with electronic [health record]... They were able to show them, there's other ways you can do the same thing.”

Organizational Preparedness

The final section of the interview involved questions related to organizational preparedness. Topics covered in this portion of the interviews included barriers that exist to being more prepared for cyber events and best practices to better preparing an organization for cyber threats.

When asked about barriers to being more prepared, there were three main topics the participants mentioned. The first barrier they felt exists to being more secure in healthcare is the complexity of an IT network itself. As discussed above, health systems are made up of applications and products that are developed by third parties. Each health system is also different from one another. This complexity makes it hard to keep each piece of the puzzle secured. One of the administers point out,

> “There's no uniformity, and so that tremendous amount of variation in what is used and the particular brands and the particular versions. There's such variation that there is no one size fits all and I think that makes it much harder to be able to prepare for this and to prevent it from happening.”

Another barrier discussed was one often seen in Healthcare Preparedness, limited funds and limited time (Cagliuso, 2014b). There are a lot of IT solutions that could all be implemented at a facility to make it as secure as possible, however each of these solutions comes with an associated cost. Most healthcare organizations are not able to spend unlimited amounts of

money on IT solutions. There also needs to be a lot of time spent to thinking of solutions and on education of staff. One of the administrators pointed out,

> "Organizations do not have the money to do everything they want to do to prevent this from happening and to do all of the education that needs to happen on a continual basis in order to help prevent a future."

Often smaller healthcare facilities do not have a full-time emergency manager, but rather add this as a supplemental duty to another job. This was a topic brought up by one of the level-one trauma centers while considering their neighboring hospitals.

Along with limited funds affecting the ability to purchase IT solutions, so too does healthcare organizations being run as businesses. The bottom line or profit margin are important to these organizations, and there is the need to prove wanted solutions will provide good return on investment. This was expressed by a few different participants. While administrators feel it is important to invest in security, they also express that return on investment is essential. The emergency managers expressed their feelings that there is not enough data out there to effectively illustrate the vulnerabilities in healthcare. One of them also expressed his interest to frame the risk these cyber threats pose to revenue streams within the organization to get more administrators on board with costly IT solutions.

> *"*I do think we dedicate a fair portion of resources to cybersecurity….we could probably spend substantially more. The tough part is, you know, everything when it comes to resources is, you know, you have to make risk benefit decision."

Hospital executives from all departments must agree the cost of what's at stake during cyber-emergencies, i.e. patient care, private data, and business reputation, are all too much of a risk not to invest in stronger cyber-preparedness efforts.

Responsive Actions

Due to each of these facilities experiences with cyberattack, they made investments of both time and money to improve their security systems. One of the first things mentioned by facilities was the general security practices, such as more frequent password changes and use of two-factor authentication. One of the facilities went as far as not giving system access back to many employees. They reevaluated who needs access to their network to complete their daily assignments and only gave accounts to individuals who needed them. These organizations have also questioned which applications are essential to their providers. Applications that were providing duplicate functions or were not deemed essential were not restored in the system.

Another change made by the facilities was restructuring their networks. One facility created a tier structure for their applications. Tier zero is a level someone must be physically in the building to gain access to and contains highly sensitive applications. Tier one contains applications, such as the EMR and clinical data. Individuals can gain remote access to this tier but must go through the upgraded security features listed above. This tier structure has one-way traffic, so individuals can only go down the tiers to access data but cannot travel up to higher levels without access.

An additional investment in network security made by all three facilities was more education and training for staff members on how to be secure. This training includes advice for safe-cyber practices in both the professional and personal realm and is held during new staff orientations. One hospital mentioned also conducting department specific training on cyber security as a follow-up. All three organizations run phishing drills with their staff where a fake phishing email is sent out with a link to see how many staff members click the link. In the cases where staff members click on the link, some type of continued education is provided to reiterate

to them the importance of being cautious when clicking links or opening attachments. The organizations also made changes to their downtime procedures to resolve some of the issues discussed above. They keep paper copies of downtime forms, and at least one of the facilities has held a table-top drill to practice their new downtime procedures.

Finally, the participants discussed more drastic measures their organizations have taken to be more prepared for additional cyber threats. One of the HCOs developed an IT specific Incident Command Team. This team consist of a broad background of IT professionals who will respond quickly to mitigate another potential attack. If there is a question of another incident occurring, they will investigate and have the authority to immediately shut the network down if they feel it is necessary. The other two facilities discussed their use of cyber insurance. This is a specific type of insurance organizations can get to protect themselves if an attack does happen. Both HCOs had their insurance prior to their attack and discussed the insurance firms sending cyber-representatives to help with the mitigation and recovery. This is an avenue that some HCOs may be interested in and financially able to pursue, but it should not be the only solution for HCOs in preparing cyber threat. These healthcare attacks are only expected to increase in frequency over the next few years and with patient safety and data is on the line, HCOs need to invest in prevention and preparedness for their networks.

Discussion

Data collected through stakeholder interviews document the experiences of healthcare organizations responding to and recovering from a successful malware attack. There were similarities among the organizations' cyberattacks but there were also many differences. Each organization is unique in its own complex way and learning more details about attacks against healthcare can help educate the industry on what risk the threat poses. Each facility highlighted their information technology staff's quick response time to reported issues and their decision to shut everything down as essential to minimizing the viral impact on the network. While the

malware did cause large impacts across each network, none of these cases suffered data breaches. All three organizations agreed this incident was unlike any other healthcare emergency they've handled before. A malware attack is different in both its length and breadth of impact. The participating organizations operated in incident command for an extended time, which is not a normal routine for healthcare facilities. A normal emergency for healthcare usually lasts a few hours to potentially a few days; in two of the cases their recovery efforts took months. Each organization also stated their scale with regard to downtime procedures was incorrect. Their system and their staff were not prepared to lose everything at one time and to be disconnected from all digital applications for an extended time. The participating facilities acknowledgment their younger generation staff members not knowing pen and paper procedures and highlighted a gap that is taking place within the current healthcare educational environment. It is essential for staff to understand these procedures to ensure safe care and curriculum in all healthcare education need to include this information. The attack made clear how dependent on technology healthcare delivery has become.

Another topic discussed by participants was the strategy to 'just be better' than the next facility within healthcare security. This approach assumes hackers are hitting certain facilities and give up on that organization when they can't break in to the network. The attack campaigns are more random, and hackers send out numerous attempts to separate facilities at one time to see where they can get through. The attackers may then make changes to their code and could potentially send this new attempt out to the same facilities. As one of the administrators pointed out in their interview, just because a healthcare organization's defense worked today does not mean it will work tomorrow. This safety strategy boils down to passing the buck and is a faulty strategy for healthcare organizations to rely on to keep their organizations secure and their patients safe. Passing the buck on safety often leads to bigger disasters down the road (Barnier, 2011). It is not enough for safety programs to be the absence of bad things happening

but must be the presence of a plan or preparedness actions in place to prevent the attack from occurring. Through this experience, the three HCOs determined investments needed to be made to their IT security, to their staff training and awareness, and to their preparedness and response plans.

This study provided valuable insight in to hospitals' experiences during malware attacks. One limitation of this research lies in the nature of the topic itself. The healthcare industry is very private about these attacks due to patient care concerns and business reputation concerns. Stakeholders from each of the three facilities expressed the idea that more openness across healthcare regarding cyber threats is essential to being a better prepared and a more secure industry. Even with this belief, there is still the potential that the participants kept some aspects of their organizational experience private. Federal regulations similar to CMS Emergency Preparedness Rule or DHHS data breach reporting rule may be needed to open the industry up and gain access to important data. A central repository for data on malware attacks against healthcare would be vital to understanding the risk these threats pose. Until the industry is more open with information, studies like this may not be getting the full picture of actions healthcare organizations are taking to be prepared. Another potential limitation with this study is the interviews were all conducted more than a year after the incident in question. This lag of time from the organizational attack and recovery efforts to the interview could have potentially introduced bias in to the data. One observation made while analyzing the interview transcripts was not all the stakeholders from a facility reported the same experiences, but it was unclear whether these differences came from recall bias or from privacy concerns related to the incident. A few of the participants were able to pull documents from the time of the incident to confirm facts they were stating. A final limitation with this study is the data collected during these interviews may not be generalizable to all cyberattacks against healthcare in the United States. There are many different types of cyberattacks, and each attack is its own unique case

dependent on the type of attack and how far a virus permeates a network. In the previous content analysis by the authors, it was reported that six organizations reported making a ransom payment to end their attack. This was not always the case, but one could assume their experiences were much different than the ones described in this study. The data collected in this study is still vital to understanding what happens during a malware attack against a hospital and how that hospital responded.

Cyberattacks against healthcare facilities are only expected to continue to increase in frequency. In 2017, the healthcare industry became the most popular target for breach attempts (Columbus, 2018). It is clear based on the previous content analysis that most of these attacks go unreported. The participants of this study expressed the need for solid data on number of attacks as well as on the impact being seen across the industry from cyberattacks. Because the data is not being reported, there is not a central public database housing this information similar to the public database for healthcare data breaches. This study provides a detailed explanation of the impacts seen during three separate cyberattacks. Impacts could be seen with business administration, patient care, and environmental regulation. The accuracy of patient data used to make care decisions was a major concern for all the facilities during the attack. If this data had not been accurate, grave errors could have been made. Another growing concern in healthcare security is targeting of active medical devices. While none of the facilities interviewed saw impacts to their medical devices, one of the facilities does have I.V. pumps connected to their network that could have been infected with malware. If medical devices become infected, hackers could change medication dosage information or hold individual patients' lives hostage while demanding ransom from the organization (Ayala, 2016).

There is limited research on these attacks; a 2017 literature review on the topic found only 31 articles, most of which were news articles (Kruse, Frederick, Jacobson, & Monticone, 2017). An article from the American Public Health Association estimates that cyberattacks will

cost the United States Healthcare system an estimated $305 billion in revenue over the next five years (Krisberg, 2017). As highlighted in the interviews, showing the return on investment is essential to gaining buy-in from those at the top. As one of the administrators said, “Making it relevant to the individual is what matters. Not making it relevant to the organization. I think like many organizations, you have a lot of priorities that compete to be first, only one thing can be top priority.” With patient safety and the environment of care at risk, let’s hope the top priority has become a more secure digital healthcare environment.

References

Ayala, L. (2016). Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention. Berkely: Apress.

Barnier, B. (2011, Oct 25). Good risk management means no buck-passing. Harvard Business Review. Retrieved from https://hbr.org/2011/10/good-risk-management-means-no

Cagliuso, N. V. (2014a). Stakeholders' experiences with US hospital emergency preparedness: Part 1. *J Bus Contin Emer Plan*, 8(2), 156-168.

Cagliuso, N. V. (2014b). Stakeholders' experiences with US hospital emergency preparedness: Part 2. *J Bus Contin Emer Plan* , 8(3), 263-279.

Columbus, L. (2018, Oct 14). The current state of cybersecurity shows now is the time for zero trust. Forbes. Retrieved from https://www.forbes.com/sites/louiscolumbus/2018/10/14/the-current-state-of-cybersecurity-shows-now-is-the-time-for-zero-trust/#342e11da5f15

Creswell, J.W. (2007). Qualitative inquiry and research design: choosing among five approaches, 3rd ed. Thousand Oaks, CA: Sage Publishing, Inc.

United States Department of Health and Human Services Office for Civil Rights. (2016). *Breaches affecting 500 or more individuals* [data file]. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

United States Department of Health and Human Services Office for Civil Rights. (2015). *Submitting notice of a breach to the secretary*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

Healthcare IT News & HIMSS Analytics. Healthcare IT News and HIMSS Analytics quick HIT survey: Ransomware, 2016. Retrieved from https://healthmanagement.org/c/it/news/ransomware-attacks-hit-three-quarters-of-hospitals-without-them-knowing

HIMSS North America (2018). 2018 HIMSS cybersecurity survey. Retrieved from https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf

Krippendorff, K. (1989). Content analysis. In E. Barnouw, G. Gerbner, W. Schramm, T.L. Worth, & L. Gross (Eds), *International encyclopedia of communication* (Vol 1, pp. 403-407). New York, NY: Oxford University Press.

Krisberg, K. (2017). Cybersecurity: Public health increasingly facing threats. *The Nation's Health,* 107 (8), 1195.

Kruse, C.S., Frederick, B., Jacobson, T., & Monticone, D.K. (2017). Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care,* 25, 1-10.

Siwicki, B. (2017 Apr 18). Hackers hit 320% more healthcare providers in 2016 than in 2015, per HHS data. *Healthcare IT News*. Retrieved from https://www.healthcareitnews.com/news/hackers-hit-320-more-healthcare-providers-2016-2015-hhs-data

Figures and Tables

Table 1: Hospital Demographics

Hospital Name	Type of Hospital	Level of Care	Location*	Range of Beds
A	Medical Center	Level One Trauma	Urbanized Area	More than 300
B	Community Hospital	Acute Care	Rural	Between 100 and 300
C	Medical Center	Level One Trauma	Urban Cluster	More than 300

*Location Classification based on United States Census Bureau: Urbanized Areas have population over 50,000 ; Urban Clusters have population between 2,500 and 50,000 ; Rural Areas have less than 2,500. Retrieved from https://www.census.gov/geo/reference/urban-rural.html

Table 2: Participant Demographics

Participant	Hospital	Role	Job Title	Sex	Years in Field	Highest Education
1	A	Administrator	Chief Quality Officer	F	10	Masters
2	A	IT	Chief Information Security Officer	M	15	Associates
3	A	Emerg Mgmt	Emergency Manager	M	14	Registered Nurse
4	B	Administrator	V.P. Patient Care Services	F	7	Masters
5	B	IT	Director of IT Systems	M	10	Masters
6	B	Emerg Mgmt	Emergency Preparedness Coordinator	M	10	Registered Nurse
7	C	Administrator	Chief Operating Officer	M	8	Doctor of Medicine
8	C	IT	Chief Information Security Officer	F	3	Masters
9	C	Emerg Mgmt	Safety Director	M	26	Masters

Appendix

Appendix 1: Cover Letter for Interview Participants

Dear Participant,

This letter is a request for you to take part in a dissertation research project to assess cyberthreats to healthcare organizations. The objective of this project is to catalog existing cyber threats hospitals face, to test whether hospitals' all-hazards plans are sufficient to respond to and recover from malware attacks, and to expand their knowledge of organizational preparedness and mitigation of these threats. This project is conducted by Lauren Branch, doctoral candidate in the School of Public Health at West Virginia University, with the supervision of Dr. Warren Eller, an associate professor in the Department of Health Policy, Management, and Leadership. Your participation in this project is greatly appreciated and will take approximately an hour to complete the interview.

Your involvement in this project will be kept as confidential as legally possible. All data will be reported in aggregate. You must be 18 years of age or older to participate. I will not ask any information that should lead back to your identity as a participant, nor will I report information that may identify your organization. Your participation is completely voluntary. You may skip any question that you do not wish to answer, and you may discontinue at any time. IRB approval has been obtained, and a copy of approval can be provided upon request.

I hope that you will participate in this research project, as it could be beneficial in understanding cyber threats hospitals face and identifying key preparedness action areas to secure the healthcare environment. The long-term goal of my research is to improve the state of cybersecurity within the field of healthcare. Thank you very much for your time. Should you have any questions about this letter or the research project, please feel free to contact Lauren Branch at 410-440-0479 or by e-mail at lbranch@mix.wvu.edu. You can also contact Dr. Warren Eller at 304-293-0404 or by e-mail at weller@hsc.wvu.edu.

Thank you for your time and help with this project.

Sincerely,

Lauren Branch

Phone: 304-293-7073
Fax: 304-293-3098
http://oric.research.wvu.edu

Chestnut Ridge Research Building
886 Chestnut Ridge Road
PO Box 6845
Morgantown, WV 26506-6845

Appendix 2: Interview Protocol

Date: _____ Time: _____ (Start) _____ (End)

Interviewer: _____ Interviewee: _____

Thank you for agreeing to take time out of your schedule to meet with me to discuss your organizations response to and recovery from a malware attack. Your personal and organizational involvement in this project will be kept as confidential as legally possible. All data will be reported in aggregate. IRB approval has been obtained for this project, and a copy of approval can be provided upon request. You have been provided an informational cover letter via email to further explain this research project. If you wish to continue with the interview, please reply with a verbal 'yes'.

- ☐ Interviewee Consented
- ☐ Interviewee Did Not Consent. The Interview is Over.

Just a note before we get started, it is okay if you do not know the answer to some of these questions. Also, please don't feel like you have to answer every question. If there is a question you don't know or don't feel comfortable answering, please let me know and we will skip to the next question.

Domain	Questions	Probes
Demographic Information	Department: Administration, Information Technology, Emergency Management Gender: Male, Female, Other How long have you been in this field? Training for Job	What field did you work in prior to this? A degree program? Any special certifications? Experience with the type of tasks?
Issue Salience	How important is this issue to you?	Is it something you would like to dedicate more time and resources to preparing for? Is it something you think about as a major vulnerability to your system?

	What is your level of concern about this topic? (On a scale from 1-10) Do you hear people talking about this more or less now?	More or less since your attack? What about colleagues at other systems talking about this type of threat?
Situational Awareness	Please explain a little about the sequence of events when your organization realized this was a malware attack. What did your initial response time look like?	How did your organization realize they were infected with malware? Do you know how long the virus was in the system before it was realized?
System Impact	Please explain how the malware impacted your hospital. How much of an impact did this have on your system?	How many hard drives were affected within your organization? What major applications were lost? Were any patient appointments impacted?---Surgery, Inpatient, Outpatient? Was your data restore from backups? How recent were the backups? What about other systems, like security cameras? Was more than one hospital impacted?

		Were there any ambulatory care centers impacted?
Recovery/Business Continuity	What was the period to get back to normal business? How this response compared to other all-hazard responses? Was your all-hazards plan sufficient to handle the response to cyber-attack?	How many individuals were responding to this attack? • Staff from your facility • Staff from a health system • Staff from vendor companies What about this event made it different or the same? Do you see this threat as different or the same to other hazards? If different, what would you change to be more suited for this type of threat?
Organizational Preparedness	What were your organization's preparedness efforts before the attack? What were your organization's preparedness efforts after the attack? Have there been any other attacks on your organization?	Cyber security training? Sending test phishing emails to employees? Creating a cyber response plan? If so, what sort of impact on the system did they have?

	Do you feel there are barriers to preparing for this type of threat? How do you think these barriers could be overcome?	

Well that concludes all the questions I have, is there anything else you would like to add? Have I missed anything about your hospital's event that you think is important for me to know?

Thanks again for taking the time to let me interview you today.

IV. Chapter 4

Perceptions of Hospital Emergency Preparedness for Cyber Threats: A Statewide Survey

Authors:
Lauren E. Branch[1]
Warren S. Eller[2]
Tom K. Bias[3]
Michael A. McCawley[1]
Douglas J. Myers[1]
Brian J. Gerber[4]
John R. Bassler[5]

Affiliations:
[1]Department of Occupational & Environmental Health Sciences, West Virginia University, Morgantown, WV 26506, USA
[2]Department of Public Management, The City University of New York, New York, NY 10019, USA
[3]Department of Health Policy, Leadership & Management, West Virginia University, Morgantown, WV 26506, USA
[4]School of Public Affairs, Arizona State University, Phoenix, AZ 85004, USA
[5]Department of Biostatistics, University of Alabama at Birmingham, Birmingham, AL, USA

Abstract

Introduction: The healthcare industry has recently become the number one target for cyberattack in the United States. As an industry, healthcare has become extremely dependent upon digital technologies for care delivery. Cyberattacks threaten healthcare delivery and put patient lives and data at risk. Federal requirements from the Centers for Medicare and Medicaid Services on emergency preparedness help ensure hospitals' abilities to respond to hazards while continuing to provide patient care. How hospitals are applying to this mandate to cyber hazards against their organizations remains unclear, but evidence shows healthcare remains vulnerable.

Methods: A survey tool was developed to assess organizational preparedness and individual perceptions of preparedness for cyberattack. The survey was sent out to all emergency management/safety professionals within a statewide hospital association. Descriptive statistics were used for the survey variables to provide insight into organizational readiness.

Results: The response rate was 29.7% (n= 27) for emergency management/safety professionals. Most (63%) emergency management respondents reported having cyber-specific response protocols. However, only a third of the same population reported having both an all-hazards plan and a continuity of operations plan that could be used for cyber incidents, although both are required by Centers for Medicare and Medicaid Services. Almost 30% of participants responded with not confident or only somewhat confident that their organizations could handle cyber threats against their systems. The top barrier to organizations being more prepared for cyber threats was lack of financial resources.

Discussion: Participants of the survey felt confident in their individual and organizational abilities to respond to a cyberattack, but when asked about their organization's concrete preparedness actions their answers were not as strong. While completing the survey participants may not have wanted to appear vulnerable and selected answers with higher confidence than they felt. Research shows this threat will continue to evolve and increase over time. Healthcare must take steps to be more secure as an industry, including increased IT security and increased emergency management procedures. While healthcare remains vulnerable, so too does patient data and safety. It is essential for the healthcare industry to invest heavily in cybersecurity and preparedness to protect patients from these attacks.

Introduction

In 2015, healthcare became the number one targeted industry for cyberattack (Morgan, 2016). The healthcare industry became into a prime target largely due to valuable health data which can be sold for a profit and their dependence on digital technology for patient care make them more likely to pay ransom (Luna, Rhine, Myhra, Sullivan, & Kruse, 2016). There were over 100 million healthcare records breached in 2015 (Morgan, 2016). Then in 2016, cyberattacks on healthcare started to include ransom demands. The first ransomware attack on a United States hospital occurred when hackers shut down access to the hospital's digital network and demanded a ransom payment for the decryption key. After a two-week standoff, the hospital made the ransom payment to regain access to their systems. Since this initial attack, the healthcare industry has seen an increase in attacks, and the attempts against them are only expected to increase (Radke, Waters, Cleary, Evans, & Kittle, 2016).

Cyberattacks against this industry threaten healthcare delivery as well as patient safety (Ayala, 2016). A global ransomware attack in 2017 left hospitals across Great Britain locked out of their systems and the National Health Service was forced to cancel patient appointments and divert patients to unaffected emergency rooms (Graham, 2017). This attack and the effects seen in Great Britain were said to have put patients' lives directly at risk (Chappell & Neuman, 2017). One worry for future attacks is the vulnerability that exists with medical devices. On average, one hospital room has up to 20 networked devices, and larger hospitals can have around 85,000 connected devices (Silverman, 2018). Healthcare IT professionals express their concerns for these devices because they were designed by vendors who do not necessarily have security in mind. These devices can serve as point of entry in to the network for hackers to gain access to health data or to alter the devices intended purpose (Ayala, 2016).

To ensure healthcare organizations (HCOs) are prepared for different hazards that threaten patient care, the Centers for Medicare and Medicaid Services (CMS) developed

Emergency Preparedness requirements that Medicare and Medicaid service providers must follow. As part of this regulation, providers are required to conduct a risk assessment and develop an emergency plan related to their top hazards, as well as to provide staff training and testing of their emergency plans annually (Centers for Medicare and Medicaid Services, 2018). This emergency preparedness regulation is meant to ensure HCOs are ready to handle hazards that can impact their organizations while still providing care to the patients in their facilities and in their communities.

Even with these federally mandated requirements in place, the healthcare industry has not given enough credence to cyber threats within their assessments and plans. Without an accurate representation of the risk these hazards pose to healthcare, the industry remains vulnerable to cybersecurity threats (Kruse, Frederick, Jacobson, & Monticone, 2017). A recent study by the authors found hospitals who went through this type of event felt it was unlike any other emergency they'd dealt with in their healthcare experiences. Respondents mentioned both the length of the event and the breadth of impact the event had on their organizations as key factors that differentiated it from other hazards. Each of the facilities interviewed now have response protocols more tailored towards cyberattack. Stakeholders also mentioned their concerns for the lack of information sharing across the healthcare industry with regards to how HCOs should best prepare for and respond to cyber hazards.

The focus of this study is to examine hospital readiness for cyber threats by asking what HCOs do to prepare for this hazard and what barriers are in place at the organizational level to increase preparedness and prevent successful attacks. Currently, the healthcare industry has become the number one target for attempted breaches, and studies have shown they are behind other industries with security and preparedness in the cyber arena (Columbus, 2018; Kruse et al., 2017). By collecting information on organizational preparedness, this study seeks to address the gap between awareness and preparedness and understanding the organizational barriers to mitigating cyber threats. A survey was created based on existing literature and

previously conducted interviews with key stakeholders to help achieve this objective. The survey was disseminated to safety/emergency management and information technology staff from healthcare organizations to measure their knowledge and their perceptions of the organization's preparedness for cyber threats.

Methods

A survey with experimental design was developed and delivered to healthcare organizations to identify readiness levels as well as barriers to preparing for a cyberattack. Survey questions were developed based on background literature, as well as information collected during the previous trend analysis and stakeholder experience studies conducted by the authors. Background conversations with subject matter experts, including hospital administrators, information technology experts, FBI agents, emergency managers, also shaped the survey questions.

The first part of the survey collected demographic information from participants including department, age, education, and years of experience. The next part of the survey measured organizational preparedness for cyberattacks based on the Centers for Medicare and Medicaid Services Emergency Preparedness Ruling. Participants were asked questions related to these requirements, such as how often their organizations are exercising their response plans, conducting staff awareness training, and doing risk assessments related to cyber vulnerabilities within their system (Graham, Shirm, Liggin, Altken, & Dick, 2006). The final part of the survey gathered the participant's perceptions of preparedness for cyber threats against healthcare. This section was broken in to two parts, the first examining participants' perceptions of their own individual preparedness and the second examining participants' perceptions of organizational preparedness (Dorn, Savoia, Testa, Stoto, & Marcus, 2007). Topics covered in both sections, related to cyberattack, included performance of duties, providing assistance and information to

staff, contacting appropriate personnel, and handling the event. A Likert-type scale was used with these questions to measure participant confidence. Finally, participants were asked to rank their organizations overall preparedness for cyber incidents and identify any barriers that exist at an organizational level to being more prepared for this type of hazard. This survey was created in REDCap, and a copy can be found in Appendix 2.

The hospital association for one state agreed to participate in the study. Staff of affiliated hospitals who work in hospital Emergency Management/Safety were asked to participate in the survey. This member group has 91 members. Due to the sensitive nature of the survey topic, the hospital association agreed to participate only if they were able to keep their member list private. The researchers created a message which included a brief introduction, the purpose of the study, and a link to the survey. The copy of the included cover letter is included in Appendix 1. This message was sent out to the Emergency Management/Safety members by the hospital association liaison. Individuals who wished to complete the survey were asked to consent by clicking on the link that took them directly to the online survey. One additional follow-up email was sent by the hospital association as a reminder to members to complete the survey.

There were also four IT participants who completed the survey. They received the survey through emergency management/safety staff who forwarded the survey email and link to ask them to participate. Although other statistical methods have been considered, the explorative nature of the hypothesis and data collection limit the scope of statistical methodology that can be applied. As the survey tool utilized is self-reported data, combined with the disparity of sample sizes among emergency management/safety and IT professionals, descriptive statistics provide insight into organizational readiness. Descriptive statistics were calculated by professional title for all elements of the survey. Missing data is reported in the tables; however, frequencies and percentages do not include missing values in the respective

calculation. All analyses were conducted using SAS 9.4. The survey results still provide valuable insight in to the perceptions of cyber preparedness across healthcare emergency management and safety professionals.

Results

There were 31 total survey respondents; 27 from emergency management/safety and 4 from information technology. The original objective of the study was to compare perceptions of preparedness between emergency management/safety professionals and information technology (IT) professionals. A healthcare IT association located in the same state as the hospital association was pursued to participate in the survey, but they ultimately declined to have their members participate. The survey had a 29.7% response rate from emergency management/safety professionals. Due to the nature of how IT professionals received the survey link, their response rate is unknown.

Respondent demographics are laid out in Table 1. The survey sample from emergency management professionals was almost equally distributed between males and females, however the information technology participants were all males. The average age of the emergency management group was 49.8 years old, whereas the average age of the information technology group was 42.7 years old. The majority of respondents either had their bachelor's degree or their master's degree (a combined 67.7% of respondents). The largest group of respondents had between 10 and 20 years of experience in their respective career fields. Table 1 also displays participants level of comfort using technology to complete daily tasks in their workplace. Most respondents said they were very comfortable using technology (64.52%), whereas 35.48% of respondents said they were either comfortable or somewhat comfortable. When the information technology participants were removed from the sample, the level of comfort dropped to 59.2% of emergency management professionals responding with very comfortable with technology use to complete daily job duties.

Organizational Preparedness

This portion of the survey addressed federally mandated emergency preparedness requirements, as well as preparedness actions taken by the organizations to be more secure against cyber threats. Results from this portion of the survey can be found in Table 2. More than a quarter of emergency management participants (25.9%) and a quarter of information technology participants responded their organizations did not or only somewhat have enough resources to address cybersecurity concerns.

There are different types of emergency plans that healthcare organizations use, an all-hazards plan and a continuity of operations or business continuity plan, both required by CMS (Centers for Medicare and Medicaid Services, 2018). Both plans ensure healthcare providers can handle hazards that occur and get back to normal business in order to continue providing patient care and serving their community. Only a third of emergency managers responded with having both plans capable of being used for cyber events. Eight of the respondents (29.6%) said that in addition to these two plans, they also had cyber-specific response protocols. Twelve of the respondents (44.4%) only selected one of the plan options for their organization.

Another requirement from CMS is for emergency plans to be drilled or exercised annually (Centers for Medicare and Medicaid Services, 2018). Nearly half of the participants said their organizations have either never drilled or exercised a cyber scenario or they did not know whether their organization had done so (48.1%). When asked about another Emergency Preparedness Requirement, staff awareness training, two thirds of respondents said their organizations either never had training or had annual training. During a previous study, IT and Emergency Management stakeholders expressed how often the field of cybersecurity is evolving and how it only takes one employee to have poor cyber-habits to let a hacker in to the

system. The organizations from that project had been victims of malware attacks, and as part of their preparedness actions moving forward increased the amount of training they provide to staff to increase their overall security. The final requirement of the Emergency Preparedness Ruling addressed in this survey is the need to conduct a facility risk assessment. Survey respondents overwhelmingly (70%) replied their organization includes cybersecurity in their facility risk assessment at least annually.

Perceptions of Preparedness

The perceptions portion of the survey utilized Likert Scale questions to obtain the respondents' perceptions of cyber preparedness both as an individual and how they perceive their organization's preparedness level. The questions throughout this section appear to receive similar results. On an individual level, most respondents said they were either somewhat confident or confident they could perform their response duties, provide information to others in the organization, and handle the event within their department (Table 3a). The outlier of these questions was whether the respondents would be able to contact the appropriate personnel to activate their organization's emergency response protocols. Almost all the respondents (87.1%) expressed they were either confident or very confident with activation protocols. This increased level of confidence could be due to activation of hospital emergency response protocols generally being the same for all hazards, and individuals feel confident in notifying the appropriate personnel from previous experiences.

Generally, the respondents answered the same for the questions related to organizational preparedness (Table 3b). Between 19% and 30% of emergency management respondents selected somewhat confident to all questions, and between 50% and 70% of the same group selected confident. The IT respondents on the other hand reported between 75% and 100% they were confident or very confident in their organizational preparedness levels. One interesting observation in this survey section is that 29% of respondents answered not

confident or somewhat confident regarding their organization ability to handle cyber threats that threaten their network. This question received lower confidence rating that the other organizational preparedness questions, even though the other questions are all related to the ability for their organization to respond to a cyber threat.

Participants were also asked to rate their organization's overall preparedness for a cyber incident. A third of respondents rated their organization's overall preparedness as either not prepared or only somewhat prepared (Table 3c). When asked whether their organization had experienced a significant security event in the last 12 months, the majority of respondents (83.9%) answered they had not (Table 2). It is possible that this experience could impact their levels of confidence regarding their individual and organizational abilities to respond to cyberattack. In future research, a larger sample size may be able to show whether experiencing a cyberattack has an impact on confidence levels related to organizational readiness.

Barriers

The final question of the survey asked participants what barriers to their organizations ability to be more prepared for cyberattacks (Table 3c). The list of barriers was adapted from the Healthcare Information and Management Systems Society (HIMSS) Cybersecurity Survey. (HIMSS North America, 2018). Five of the top six selected barriers from the HIMSS Survey were chosen for this survey. The choices were selected based on answers to a barriers question during the stakeholder research project. The top two barrier selections from the HIMSS survey swapped places with our survey respondents. The highest rated barrier selected by respondents was lack of financial resources. While this is not a new theme for barriers of hospital emergency preparedness, this was an interesting observation in this population because in Part 2 of the survey only 6.5% of respondents felt their organization did not have enough resources to address cybersecurity concerns (Cagliuso, 2014). The second most selected barrier was lack of appropriate personnel. In the previous study by the authors,

stakeholders noted a concern was lacking a full-time employee dedicated to emergency management at many facilities. The stakeholders also noted the struggle of IT departments to stay on top of the constantly evolving cyber security front. Related to the ever-changing nature of this threat, the third most selected barrier was too many new and emerging threats. While barriers to healthcare emergency management exist for all hazards, healthcare has become the number one industry targeted for cyberattack. To protect patient care and protected data, hospital administrators must realize how essential the roles of emergency management and information technology departments are to keep their systems secure.

Discussion

Data collected from this survey document participants perceptions of preparedness for cyberattack within their healthcare facility. Overall, the survey results showed high confidence levels in individual ability and in organizational ability to respond to a cyberattack. Almost all respondents (87.1%) said they were confident or very confident in their ability to contact the appropriate personnel for event response activation. Regarding performance of individual response duties, 80% of participants answered they were either confident or very confident in their own ability. Most participants (73.3%) answered confident or very confident in their organization's ability to secure their system during a cyberattack, and eighty percent of participants gave the same answers regarding their organization's ability to ensure continuation of patient care without digital technology.

While the respondents answered with relatively high confidence levels about their preparedness perceptions, when asked about their organizations actions to be prepared for cyber threats a few disparities became apparent. Only a third of survey participants reported having an all-hazards plan and a business continuity plan that could be used for cyberattacks, both of which are required by CMS for all providers to ensure the ability to handle hazards and

safeguard continuation of care. While the question was related specifically to use against cyber hazards, the CMS requirements are meant to guarantee hospitals can protect patient care during any emergency event. Without the ability to use their emergency plan during a cyberattack, it is unclear if the hospitals questioned have a plan to respond while safeguarding patient care. Another discrepancy across survey responses was 74.1% of individuals reported their organization had enough resources to address cyber security concerns, yet when asked about barriers to being more prepared respondents' top choices were lack of financial resources and lack of appropriate personnel.

This study provided valuable insight in to the preparedness actions of healthcare facilities and stakeholders' perceptions of their organizational ability to respond to a cyberattack. An objective of this survey, to compare perceptions between departments, was not fulfilled due to the small sample size. The IT organization may have declined to participate due to the private nature of cyberattacks and the concern to admit vulnerabilities exist within the state. This same concern was expressed by the participating hospital association, however they were willing to participate as long as the association and its members could remain anonymous. While this survey had an average response rate for an online survey, the results may not be generalizable to all organizations statewide (Nulty, 2008). Future research efforts need to focus on expanding the size of the sample population as well as gain more participation from association members. It is also important to note that the survey questions were collecting information on the respondent's perceptions of readiness to respond to a cyberattack and to continue providing patient care during an attack, but most facilities haven't experienced a cyber attack. Only 16.1% of respondents reported their organizations having had a significant security incident in the past 12 months. Previous research has shown individuals who experience a cyberattack express a change in their understanding of what happens during attacks within healthcare organizations. This would be another variable to consider comparing

preparedness perceptions across within a larger sample size. Finally, due to the sensitive nature of this threat healthcare organizations across the country are choosing to keep information private. This was a concern expressed by both professional groups approached to participate in this research project. This desire to keep data confidential may have led to response bias in the survey results. Respondents could have reported higher confidence levels not wanting their organization to seem vulnerable to such attacks. This response bias could explain the differences seen between perceptions of preparedness and the preparedness actions seen across the participant organizations.

Even though the participants in this survey reported feeling relatively confident in their organizations ability to respond to a cyberattack, previous research has shown individuals in healthcare are less confident overall about their system security and ability to respond to attacks. A recent survey of Health IT professionals found that 60% were not confident in their medical devices security strategies to protect patient care (Silverman, 2018). It is also apparent that healthcare remains vulnerable (Kasumov, 2018). Healthcare Organizations have continued to be targeted and in 2018 there have been large scale cyberattacks against hospitals, healthcare providers, and third-party healthcare vendors (Duffy, 2018). During these attacks, the reliability of all health data becomes questionable. Organizations and providers must find out if the information they are seeing is accurate or has it been altered in some way, including data from patient records, diagnosis equipment, and treatment equipment (Ayala, 2016). Without accurate patient records and histories, patient care can be put at risk (Lachance, 2016).

This category of threat is different in nature than any other threat healthcare handles. Healthcare is used to a certain level of downtime, but previous studies have shown this is unlike any downtime they have prepared for. During cyberattacks, every digital device and application within the facility can go down at one time and there is the potential for these to remain offline for an extended period. To be prepared, HCOs need to include cyber hazards when conducting

risk assessments and to reevaluate emergency plans to ensure they account for these cyber incidents. It is essential for hospitals to have plans in place to ensure continuation of care and patient safety during this level of downtime. HCOs also need to develop an exercise and drilling plan to practice their cyber procedures with employees, as well as strengthen their training programs with staff members to ensure their staff know what to do and how to remain vigilant (Rafee, 2018). The banking industry used to be the number one targeted area for cyberattacks in 2014, but after a surge in their cybersecurity budgets banking dropped down to number three in 2015 (Morgan, 2016).

The healthcare industry itself is also changing and becoming even more dependent on a digital environment. With new delivery avenues becoming more popular, such as telemedicine and patient portals, the attack surface within the field is expanding (Adefala, 2018; Sullivan, 2018. This threat against healthcare is not disappearing, and cyberattacks are expected to increase (Duffy, 2018). Barriers identified by study participants include lack of financial resources and lack of appropriate personnel. Federal funding for the Hospital Preparedness Program has been cut by 50% over the last 15 years from $515 million in FY2003 to $255 million in FY2017 (Watson, Watson, & Sell, 2017). There is a need for sustained federal support for hospital emergency preparedness to sustain their response capabilities. Another source of funding could come from the healthcare organizations themselves. Currently, healthcare is the now the second biggest sector of the United States' economy, yet the healthcare industry only spends about half on cybersecurity as other industries (Silverman, 2018). Cases need to be made for the return on investment (ROI) to advancing cybersecurity resources (Adefala, 2018; Rafee, 2018). Data about the risk and impact of cyberattacks needs to be made more readily available for healthcare. This data along with identification of best practices from case studies can be used to make ROI cases to hospital administrators. The healthcare industry needs to become more open about these attacks to identify best practices

and pool their preparedness resources. These attacks will continue to get more sophisticated and continue to threaten patient care and safety. Research has shown all devices in the healthcare setting are at risk of being infiltrated and altered. The healthcare industry is charged with doing no harm to the population they serve, and to do nothing for such a clear threat is irresponsible.

References

Adefala, L. (2018, Mar 6). Healthcare experiences twice the number of cyber attacks as other industries. CSO. Retrieved from https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

Ayala, L. (2016). Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention. Berkeley: Apress.

Cagliuso, N. V. (2014b). Stakeholders' experiences with US hospital emergency preparedness: Part 2. *J Bus Contin Emer Plan*, 8(3), 263-279.

Centers for Medicare and Medicaid Services. (2018). Core EP rule elements. Retrieved from https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Core-EP-Rule-Elements.html

Chappell, B. and Neuman, S. (2017, Dec 19). U.S. says North Korea 'directly responsible' for wannacry ransomware attack. *NPR*. Retrieved from https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

Columbus, L. (2018, Oct 14). The current state of cybersecurity shows now is the time for zero trust. Forbes. Retrieved from https://www.forbes.com/sites/louiscolumbus/2018/10/14/the-current-state-of-cybersecurity-shows-now-is-the-time-for-zero-trust/#342e11da5f15

Dorn, B.C., Savoia, E., Testa, M.A., Stoto, M.A., & Marcus, L.J. (2007). Development of a survey instrument to measure connectivity to evaluate National public health preparedness and response performance. *Public Health Rep*, 122, 329-338.

Duffy, M. (2018 Jan 30). Cyber attack evolution in 2018: 3 key trends for healthcare organizations. Becker's Hospital Review. Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/cyber-attack-evolution-in-2018-3-key-trends-for-healthcare-organizations.html

Graham, C. (2017, May 20). NHS cyber attack: everything you need to know about 'biggest ransomware' offensive in history. Daily Telegraph. Retrieved from https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

Graham, J., Shirm, S., Liggin, R., Altken, M.E., & Dick, R. (2006). Mass-casualty events at schools: A National preparedness survey. *Pediatrics,* 117(1), e8-15.

HIMSS North America (2018). 2018 HIMSS cybersecurity survey. Retrieved from https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf

Kasumov, A. (2018, Jul 17). Cyberattacks on health-care providers are up in recent months. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2018-07-17/cyberattacks-on-health-care-providers-are-up-in-recent-months

Kruse, C.S., Frederick, B., Jacobson, T., & Monticone, D.K. (2017). Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care,* 25, 1-10.

Lachance, N. (2016 Apr 1). Malware attacks on hospitals put patients at risk. NPR. Retrieved from https://www.npr.org/sections/alltechconsidered/2016/04/01/472693703/malware-attacks-on-hospitals-put-patients-at-risk

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C.S. (2016). Cyber threats to health information systems: a systemic review. *Technol Health Care*, 24, 1-9.

Morgan, S. (2016 May 13). Top 5 industries at risk of cyber-attacks. Forbes. Retrieved from https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#1855190a715e

Nulty, D.D. (2008). The adequacy of response rates to online and paper surveys: what can be done? *Assess Eval High Educ,* 33(3), 301-314.

Radke, B.A., Waters, M.J., Cleary, J.C., Evans, D., & Kittle, C. (2016, July 18). Ransomware rises among hospitals. Lexology. Retrieved from http://www.lexology.com/library/detail.aspx?g=8f3d29a5-2f87-42b8-ada1-54a109e38b3f

Rafee, S. (2018 Mar 16). 2018 cybersecurity trends in healthcare. IBM. Retrieved from https://www.ibm.com/blogs/insights-on-business/healthcare/2018-cybersecurity-trends-healthcare/

Silverman, L. (2018 Oct 16). How cyberhardening can reduce risk to the entire medical community. Becker's Hospital Review. Retrieved from https://www.beckershospitalreview.com/cybersecurity/how-cyberhardening-can-reduce-risk-to-the-entire-medical-community.html

Watson, C.R., Watson, M., & Sell, T.K. (2017). Public health preparedness funding: Key programs and trends from 2001 to 2017. *Am J Public Health Pub Health Prac*, 107(S2), S165-S167.

Figures and Tables

Table 1: Demographic Information

Table 1. Demographic Information				
Response Variables by Department		**Total (N = 31)**	**Emergency Management/Safety (N = 27)**	**Information Technology (N = 4)**
		Frequency (%)	**Frequency (%)**	**Frequency (%)**
Age*		48.93 (10.42)	49.85 (10.38)	42.75 (9.67)
Gender	**Male**	17 (54.84)	13 (48.15)	4 (100.00)
	Female	14 (45.16)	14 (51.85)	0 (0.00)
Education Level	**Doctorate Degree**	1 (3.23)	1 (3.70)	0 (0.00)
	Master's Degree	11 (35.48)	10 (37.04)	1 (25.00)
	Bachelor's Degree	10 (32.26)	7 (25.93)	3 (75.00)
	Associate Degree	4 (12.90)	4 (14.81)	0 (0.00)
	High School / GED	4 (12.90)	4 (14.81)	0 (0.00)
	Other	1 (3.23)	1 (3.70)	0 (0.00)
Years of Experience	**0 - 10**	6 (19.35)	5 (18.52)	1 (25.00)
	10 - 20	12 (38.71)	10 (37.04)	2 (50.00)
	20 - 30	6 (19.35)	6 (22.22)	0 (0.00)
	30 - 40	5 (16.13)	4 (14.81)	1 (25.00)
	40 - 50	2 (6.45)	2 (7.41)	0 (0.00)
How comfortable do you feel using technology in your workplace to complete your daily tasks?	**Not Comfortable**	0 (0.00)	0 (0.00)	0 (0.00)
	Somewhat Comfortable	3 (9.68)	3 (11.11)	0 (0.00)
	Comfortable	8 (25.81)	8 (29.63)	0 (0.00)
	Very Comfortable	20 (64.52)	16 (59.26)	4 (100.00)

* Summary statistics reported for age are Mean (Standard Deviation)

Table 2: Cyber Preparedness- Emergency Management Requirements

Table 2. Preparedness Information

Response Variables by Department		Total (N = 31)	Emergency Management/Safety (N = 27)	Information Technology (N = 4)
		Frequency (%)	Frequency (%)	Frequency (%)
Do you feel your organization has enough resources to address cybersecurity concerns?	Yes	23 (74.19)	20 (74.07)	3 (75.00)
	Somewhat	6 (19.35)	6 (22.22)	0 (0.00)
	No	2 (6.45)	1 (3.70)	1 (25.00)
Does your organization have an emergency plan for cyber events?	None	1 (3.23)	1 (3.70)	0 (0.00)
	Cyber-Specific Response Protocols	19 (60.29)	17 (62.96)	2 (50.00)
	All-Hazards Plan	7 (22.58)	6 (22.22)	1 (25.00)
	Continuity of Operations Plan	3 (9.68)	3 (11.11)	0 (0.00)
	Other	1 (3.23)	0 (0.00)	1 (25.00)
Does your organization drill or exercise its response to a cyber event for staff to know what steps to take to mitigate the effects of a successful attack?	Never	10 (32.26)	8 (29.63)	2 (50.00)
	Yearly	15 (48.39)	13 (48.15)	2 (50.00)
	Quarterly	1 (3.23)	1 (3.70)	0 (0.00)
	Monthly	0 (0.00)	0 (0.00)	0 (0.00)
	Do Not Know	5 (16.13)	5 (18.52)	0 (0.00)
How comfortable do you feel using technology in your workplace to complete your daily tasks?	Never	7 (22.58)	6 (22.22)	1 (25.00)
	Yearly	15 (48.39)	12 (44.44)	3 (75.00)
	Quarterly	6 (19.35)	6 (22.22)	0 (0.00)
	Monthly	1 (3.23)	1 (3.70)	0 (0.00)
	Do Not Know	2 (6.45)	2 (7.41)	0 (0.00)
Does your organization do cybersecurity risk assessments to identify system vulnerabilities?	Never	0 (0.00)	0 (0.00)	0 (0.00)
	Yearly	12 (38.71)	9 (33.33)	3 (75.00)
	Quarterly	5 (16.13)	5 (18.52)	0 (0.00)
	Monthly	6 (19.35)	5 (18.52)	1 (25.00)
	Do Not Know	8 (25.51)	8 (29.63)	0 (0.00)
Has your organization experienced a significant security incident in the past 12 months?	Yes	5 (16.13)	5 (18.52)	0 (0.00)
	No	22 (70.97)	22 (81.48)	4 (100.00)

Table 3a: Perceptions of Individual Preparedness for Cyber Hazards

Table 3a. Preparedness Perceptions

In the event of a cyber-event, how well do you feel you will be able to:		Total (N = 31)	Emergency Management/Safety (N = 27)	Information Technology (N = 4)
		Frequency (%)	Frequency (%)	Frequency (%)
Perform response duties you will be expected to accomplish?	Not Confident	0 (0.00)	0 (0.00)	0 (0.00)
	Somewhat Confident	6 (20.00)	6 (23.08)	0 (0)
	Confident	21 (70.00)	18 (69.23)	3 (75)
	Very Confident	3 (10.00)	2 (7.69)	1 (25)
	Missing*	1	1	0
Provide assistance and information to others within organization?	Not Confident	1 (3.23)	1 (3.7)	0 (0)
	Somewhat Confident	7 (22.58)	7 (25.93)	0 (0)
	Confident	18 (58.06)	14 (51.85)	4 (100)
	Very Confident	5 (16.13)	5 (18.52)	0 (0)
Contact the appropriate personnel to activate event response?	Not Confident	0 (0.00)	0 (0.00)	0 (0.00)
	Somewhat Confident	4 (12.90)	4 (14.81)	0 (0)
	Confident	14 (45.16)	12 (44.44)	2 (50)
	Very Confident	13 (41.94)	11 (40.74)	2 (50)
Handle the event within your department/team?	Not Confident	1 (3.23)	1 (25)	0 (0)
	Somewhat Confident	6 (19.35)	0 (0)	6 (22.22)
	Confident	16 (51.61)	2 (50)	14 (51.85)
	Very Confident	8 (25.81)	1 (25)	7 (25.93)

* Missing data is not included in the calculated percentages

Table 3b: Perceptions of Organizational Preparedness for Cyber Hazards

Table 3b. Preparedness Perceptions

Presently, how well do you think your organization is able to:		Total (N = 31)	Emergency Management/Safety (N = 27)	Information Technology (N = 4)
		Frequency (%)	Frequency (%)	Frequency (%)
Perform response duties your organization will be expected to accomplish?	Not Confident	0 (0.00)	0 (0.00)	0 (0.00)
	Somewhat Confident	7 (23.33)	7 (26.92)	0 (0.00)
	Confident	20 (66.67)	16 (61.54)	4 (100.00)
	Very Confident	3 (10.00)	3 (11.54)	0 (0.00)
	Missing*	1	1	0
Provide assistance and information to staff within the main hospital?	Not Confident	0 (0.00)	0 (0.00)	0 (0.00)
	Somewhat Confident	5 (16.67)	5 (19.23)	0 (0.00)
	Confident	22 (73.33)	18 (69.23)	4 (100.00)
	Very Confident	3 (10.00)	3 (11.54)	0 (0.00)
	Missing*	1	1	0
Provide assistance and information to staff within satellite offices/ambulatory care centers?	Not Confident	0 (0.00)	0 (0.00)	0 (0.00)
	Somewhat Confident	7 (25.93)	7 (29.17)	0 (0.00)
	Confident	19 (70.37)	16 (66.67)	3 (100.00)
	Very Confident	0 (0.00)	1 (4.17)	0 (0.00)
	Missing*	4	3	1
Secure the system (i.e. stop the spread of virus)?	Not Confident	0 (0.00)	0 (0.00)	0 (0.00)
	Somewhat Confident	8 (26.67)	7 (26.92)	1 (25.00)
	Confident	17 (56.67)	15 (57.69)	2 (50.00)
	Very Confident	5 (16.67)	4 (15.38)	1 (25.00)
	Missing*	1	1	0
Ensure continuation of patient care (i.e. switch to pen and paper records)?	Not Confident	0 (0.00)	0 (0.00)	0 (0.00)
	Somewhat Confident	6 (20.00)	5 (19.23)	1 (25)
	Confident	20 (66.67)	18 (69.23)	2 (50)
	Very Confident	4 (13.33)	3 (11.54)	1 (25)
	Missing*	1	1	0
Handle potential cyber threats that threaten your network?	Not Confident	1 (3.33)	1 (3.85)	0 (0)
	Somewhat Confident	8 (26.67)	7 (26.92)	1 (25)
	Confident	14 (46.67)	13 (50)	1 (25)
	Very Confident	7 (22.58)	5 (19.23)	2 (50)
	Missing*	1	1	0

* Missing data is not included in the calculated percentages

Table 3c: Overall Preparedness Perceptions for Cyber Hazards

Table 3c. Preparedness Perceptions

Response Question by Department		Total (N = 31)	Emergency Management/Safety (N = 27)	Information Technology (N = 4)
		Frequency (%)	Frequency (%)	Frequency (%)
Overall, how would you rate your organization's preparedness level to respond to and mitigate the effects of a cybersecurity incident?	Not Prepared	1 (3.33)	1 (3.85)	0 (0.00)
	Somewhat Prepared	8 (26.67)	7 (26.92)	1 (25.00)
	Prepared	17 (56.67)	14 (53.85)	3 (75.00)
	Very Prepared	4 (13.33)	4 (29.63)	0 (0.00)
	Missing*	1	1	0
What do you feel the biggest barriers are to your organization being MORE prepared for a cybersecurity incident?	Lack of Appropriate Personnel	6 (20.00)	5 (19.23)	1 (25.00)
	Lack of Financial Resources	8 (26.67)	7 (26.92)	1 (25.00)
	Too Many Application Vulnerabilities	1 (3.33)	1 (3.85)	0 (0.00)
	Too Many Endpoints to the Network	3 (10.00)	3 (11.54)	0 (0.00)
	Too Many New and Emerging Threats	5 (16.67)	4 (15.38)	1 (25.00)
	Complex Network Infrastructure Unable to be Properly Secured	2 (6.67)	1 (3.85)	1 (25.00)
	Other	2 (6.67)	2 (7.69)	0 (0.00)
	Do Not Know	3 (10.00)	3 (11.54)	0 (0.00)
	Missing*	1	1	0

* Missing data is not included in the calculated percentages

Appendix

Appendix 1: Cover Letter to participants explaining the survey

Good Morning,

This is a request for you to take part in a dissertation research project to assess healthcare preparedness for cyberthreats to healthcare organizations. The objective of this project is to expand knowledge of organizational preparedness and mitigation of these threats. This project is conducted by Lauren Branch, doctoral candidate in the School of Public Health at West Virginia University, with the supervision of Dr. Warren Eller, an associate professor in the Department of Health Policy, Management, and Leadership. Your participation in this project is greatly appreciated and will take approximately 10 minutes to complete the survey.

Your involvement in this project will be kept as confidential as legally possible. Your survey answers will remain anonymous, and all data will be reported in aggregate. You must be 18 years of age or older to participate. I will not ask any information that would lead back to your identity as a participant, nor will I collect information that may identify your organization. Your participation is completely voluntary. You may skip any question that you do not wish to answer, and you may discontinue at any time. IRB approval has been obtained, and a copy of approval can be provided upon request.

I hope that you will participate in this research project, as it could be beneficial in understanding cyber threats hospitals face and identifying key preparedness action areas to secure the healthcare environment. Thank you very much for your time. Should you have any questions about this research project, please feel free to contact Lauren Branch at 410-440-0479 or by e-mail at lbranch@mix.wvu.edu. You can also contact Dr. Warren Eller at 304-293-0404 or by e-mail at wseller@hsc.wvu.edu.

The research survey will take approximately 10 minutes to complete. If you choose to participate and consent to being part of this research project, please click on the survey link below to complete the survey questions.

Thank you for your time and help with this project.

Sincerely,

Lauren E. Branch

Lauren E. Branch, MPH
Doctoral Candidate
West Virginia University School of Public Health
Occupational and Environmental Health Sciences

Phone: 304-293-7073
Fax: 304-293-3098
http://oric.research.wvu.edu

Chestnut Ridge Research Building
886 Chestnut Ridge Road
PO Box 6845
Morgantown, WV 26506-6845

Appendix 2: Healthcare Cyber Preparedness and Perceptions Survey

Resize font:

Healthcare Cyber Preparedness and Perceptions

This research survey will take approximately 10 minutes to complete. Your answers will remain anonymous, and all data will be reported in aggregate. Your participation is completely voluntary. You may skip any question that you d not wish to answer, and you may discontinue at any time.

When finished, please click the "Submit" button at the bottom of the survey.

Thank you for your time and help with this project.

Part 1: Demographic Information

1.1 What is your gender?

- Male
- Female

reset

1.2 What is your age (in years)?

1.3 Which of the following departments do you work in?

- Emergency Management/Safety
- Information Technology

reset

1.4 Which of the following best describes your job title?

- ( )
- ( ) Executive Management
- ( ) Non-Executive Management (i.e. midlevel or senior management)
- ( ) Non-Management (i.e. specialist, analyst, tech)
- Other

reset

1.5 How many years of experience do you have in your career field?

1.6 What is your level of education?

- ( )
- ( )
- ( ) Doctorate Degree (i.e. PhD, MD)
- ( ) Master's Degree
- ( ) Bachelor's Degree
- ( ) Associate's Degree
- ( ) High School/GED
- Other

reset

1.7 Do you have any professional certifications related to your job duties?

- ( )
- ( ) Yes
- No

reset

1.8 How comfortable do you feel using technology in your workplace to complete your daily tasks?

- ( )
- ( ) Not Comfortable
- ( ) Somewhat Comfortable
- ( ) Comfortable
- Very Comfortable

reset

Part 2: Preparedness Information

2.1 Do you feel your organization has enough resources to address cybersecurity concerns?

- ( )
- ( ) Yes
- ( ) Somewhat
- No

reset

2.2 Does your organization have an emergency plan for cyber events? (Select all that apply)

- [ ] None
- [ ] Cyber-specific response protocols
- [ ] All-hazards plan
- [ ] Continuity of Operations Plan (COOP)

Other

2.3 Does your organization drill or exercise its response to a cyber event for staff to know what steps to take to mitigate the effects of a successful attack?

- ( ) Never
- ( ) Yearly
- ( ) Quarterly
- ( ) Monthly
- ( ) Don't Know

reset

2.4 **Does your organization hold cybersecurity awareness training for staff to prevent a successful attack (i.e. how to avoid click baits)?**

- ○ Never
- ○ Yearly
- ○ Quarterly
- ○ Monthly
- ○ Don't Know

reset

2.5 **Does your organization do cybersecurity risk identify system vulnerabilities?**

- ○ Never
- ○ Yearly
- ○ Quarterly
- ○ Monthly
- ○ Don't Know

reset

2.6 **Has your organization experienced a significant security incident in the past 12 months?**

- ○ Yes
- ○ No

reset

Part 3: Preparedness Perceptions

In the event of a cyber-event, how well do you feel you will be able to:

		Not Confident	Somewhat Confident	Confident	Very Confident
3.1.1	Perform response duties you will be expected to accomplish?	○	○	○	○
3.1.2	Provide assistance and information to others within organization?	○	○	○	○

reset

3.1.3	**Contact the appropriate personnel to activate event response?**	○	○	○	○ reset
3.1.4	**Handle the event within your department/team?**	○	○	○	○ reset

Presently, how well do you think your organization is able to:

		Not Confident	Somewhat Confident	Confident	Very Confident
3.2.1	**Perform response duties your organization will be expected to accomplish?**	○	○	○	○ reset
3.2.2	**Provide assistance and information to staff within the main hospital?**	○	○	○	○ reset
3.2.3	**Provide assistance and information to staff within satellite offices/ambulatory care centers? (If this is not applicable to your organization, please leave blank)**	○	○	○	○ reset
3.2.4	**Secure the system (i.e. stop the spread of virus)?**	○	○	○	○ reset
3.2.5	**Ensure continuation of patient care (i.e. switch to pen and paper records)?**	○	○	○	○ reset
3.2.6	**Handle potential cyber threats that threaten your network?**	○	○	○	○ reset

3.3 Overall, how would you rate your organization's preparedness level to respond to and mitigate the effects of a cybersecurity incident?

- ○ Not Prepared
- ○ Somewhat Prepared
- ○ Prepared
- ○ Very Prepared

reset

3.4 What do you feel the biggest barriers are to your organization being MORE prepared for a cybersecurity incident (Select all that apply):

- ☐ Lack of appropriate personnel
- ☐ Lack of financial resources
- ☐ Too many application vulnerabilities
- ☐ Too many endpoints to the network (i.e. computers, user devices)
- ☐ Too many new and emerging threats
- ☐ Complex network infrastructure unable to be properly secured
- ☐ Other
- ☐ Don't Know

reset

Submit

V. Summary

Introduction

The United States healthcare industry has recently found itself a target for cybercriminals. As the field shifted towards electronic medical records, hackers realized they could access valuable information worth even more than identity or financial information (Yao, 2017). Since 2015, healthcare has become the number one targeted industry for cyber breaches (Columbus, 2018). There were over 1.9 million individuals impacted by reported data breaches caused by hacking or IT incident in 2017 alone (United States Department of Health and Human Services Office for Civil Rights, 2016).

A shift in cyber threats within healthcare was seen in 2016 as the first hospital was hit with a ransomware attack. Ransomware attacks are a type of cyberattack where hackers deliver a malware virus to a hospital network and can essentially lock the hospital out of their own system while demanding a ransom payment for the decryption key. Hollywood Presbyterian Hospital in Los Angeles, California was offline for over a week before settling with hackers to pay a $17,000 ransom (Winton, 2016).

Due to the growing use of electronic medical records and the increasing dependence on technology for care delivery, hospitals make a target often willing to pay to get their systems back up and running. Patient care systems that can potentially be impacted during these cyberattacks include patient history and medical charts, laboratory testing, diagnostic imaging, medication dispensing, medical devices, and treatment devices. Without access to historical data or these patient care systems providers may not be providing the best care or there could be delays in care provided. This type of attack a healthcare facility can potentially put patient safety at risk. Since this first ransomware attack against the healthcare field, the trend has only continued to grow (Radke, Waters, Cleary, Evans, & Kittle, 2016). While this hazard

continues to threaten healthcare, data are still lacking regarding frequency, impact, and recommended actions for healthcare organizations.

Summary of Key Findings

This research project was meant to serve as an exploratory study to examine an emerging threat to public health. The overall purpose was to provide descriptive data on how cyberattacks impact the four phases of the emergency cycle (preparedness, response, mitigation, and recovery) within healthcare organizations (Centers for Disease Control and Prevention, 2014). Data on publicly reported malware attacks was compiled in Study 1 (Chapter 2) to assess attack trends. Study 2 (Chapter 3) examined organizational practices on mitigation and recovery from malware attacks. Data on organizational preparedness for cyber threats was collected in Study 3 (Chapter 4). Due to this being a relatively new threat for healthcare, research on the area is limited (Luna, Rhine, Myhra, Sullivan, & Kruse, 2016; Kruse, Frederick, Jacobson, & Monticone, 2017). The data collected from the studies as part of this research project help to fill the gap in knowledge and help to elucidate the threat cyberattacks pose to healthcare.

The trend analysis of public data identified 49 malware attacks on United States healthcare providers between 2016 and 2017. Attacks occurred across 27 states, with California seeing the highest frequency at 9 attacks during the two year time frame. Forty-one of the attacks were labeled ransomware and eight of the incidents were labeled malware. Six of the organizations reported paying ransom, whereas 43 organizations did not pay or did not report payment to the press. The analysis identified a range of organizational impacts from network downtime to patient and staff records being breached. The longest downtime reported was 3 weeks, and there were four attacks that reported having more than 200,000 records breached. This was the first known content analysis to summarize malware attack trends in detail seen on United States healthcare providers, however reports from expert agencies report

higher frequencies of attacks. The Healthcare Information Management Systems Society conducts a cybersecurity survey each year and the 2018 survey revealed 75.7% of respondents reported a significant security incident in the past 12 months (HIMSS North America, 2018). While this is a large percentage, it is important to note the survey sample size was 239 healthcare organizations. Even though healthcare is facing this new threat, as an industry they remain private when choosing to report these incidents due to the nature of attack and the potential threat to patient care as well as the potential impact on the organization's business reputation for keeping information secure. This lack of reporting could explain the low number or attacks found in public sources within the trend analysis.

Study 2 (Chapter 3) used data collected from stakeholder interviews to examine organizational mitigation and recovery from malware attacks. The three organizations that participated in this study experienced complete shutdowns of their networks during their malware attack. The network outages lasted varying amounts of time based on how far the virus was able to infect their systems. Two of the organizations saw devastating impacts and were forced to operate within the incident command structure for over a month. These organizations had to rebuild their networks with a cost upwards of $10 million. Stakeholders from all categories (administrators, emergency managers, and information technology managers) expressed this event being different from any other emergency they have faced while in their healthcare careers. One of the key themes that emerged from the stakeholders interviews was the realization of how technologically dependent they have become in healthcare provision. One hospital administrator explained they are no longer able to take a blood sugar reading without access to their electronic medical record. Stakeholders expressed concern for this reliance on technology, but also expressed the benefit of technology in the health field. Stakeholders expressed frustration in the reporting privacy that exists within the healthcare field. They also identified the need for their industry to be more open with regard to cyberattack data.

Multiple interview subjects believe this data would be useful in providing more accurate risk assessments and give them the information they need to convince administrators to make system improvements to become more secure. The identification of the need to convince administration to invest in safety and emergency management solutions is nothing new to the field of hospital emergency management (Cagliuso, 2014a; Cagliuso, 2014b). However, cyberattacks create a different need for emergency preparedness solutions that is not similar to the other hazards healthcare faces.

This final study of this project (Chapter 4) expanded knowledge on organizational preparedness for cyber threats. A survey was developed and delivered to emergency managers within a statewide hospital association. The majority (63%) of emergency managers reported having cyber-specific protocols within their organization. However, only a third of respondents reported having both an all-hazards plan and a continuity of operations plan that could be used during cyberattack. Both of these plans are requirements of Centers for Medicare and Medicaid Services (CMS) and as part of the CMS Emergency Preparedness Ruling must reflect the hazards identified in the facility's thorough hazard vulnerability assessment. With only a third of emergency managers reporting having plans that address cyber threats, the other two thirds of participants must either feel they are not at risk for a cyberattack or did not consider cyber threats to their organizations while conducting their risk assessments. Also, 30% of participants responded with confidence or somewhat confident their organizations could handle cyber threats against their systems. Based on Study 2, these responses were unexpected because the participants said this was unlike any other emergency they had faced and also felt they had misjudged the impact these attacks could have on their system. When asked if their organizations could handle threats against their systems, almost 30% the survey participants reported they were not confident or only somewhat confident. Finally, the survey asked about barriers to being more prepared and the participants identified

lack of financial resources as the biggest barrier. While this is not unlike other healthcare emergency management literature, it was unexpected because when asked if their organizations have enough resources dedicated to cybersecurity 74% of emergency managers answered 'yes' (Cagliuso, 2014a, Cagliuso 2014b). Response bias may have been a factor for higher levels of confidence being reported than have been seen in other healthcare surveys. Due to the private nature of healthcare regarding this threat topic, respondents may have responded with higher confidence not wanting to make the state hospital association seem vulnerable to attack.

Discussion

News and industry reports make it clear cyberattacks pose a real threat to healthcare and are only expected to grow as a threat over time (Kasumov, 2018; Kruse et al., 2017; Luna et al.). A recent report estimated healthcare experiences twice the number of cyberattacks as seen in other industries (Adefala, 2018). The studies in this research project more clearly illustrate what threat cyberattacks can pose to the healthcare industry. Data from studies showed the frequency and impact of malware attacks as well as the steps being taken by organizations to prepare for and to mitigate the effects of attacks. Across all studies, three main points related to cybersecurity and public health preparedness were identified.

One point that appeared across all three studies was the current lack of research related to cyberattacks and healthcare organizations. A 2017 systematic review found 31 articles related to cyberattacks and healthcare and the reviewers noted most of the articles found were news articles and not academic articles (Kruse et al., 2017). Not only is there lack of research on this topic, but participants in the studies pointed out a lack of accessible data for those in the field. The Federal Bureau of Investigations (FBI) collects data related to cyberattacks across all industries. The FBI reported in 2015 they had received over 2,500 complaints of ransomware across all industries (Radke, Waters, Cleary, Evans, & Kittle, 2016). We also know they have

data because their local Fusion Centers are often called when a healthcare organizations is attacked and local agents go out to the site to assist with response and collect evidence for forensic testing. This participation by FBI agents was confirmed by participants in Study 2 when discussing their organizational response to attack. Even though the FBI has this data, inquiries to gain access to the data reports or to separate out healthcare data from other industries were often met with refusals. I experienced these refusals when talking to two separate FBI agents and stakeholders from Study 2 reported the same experiences. There is also public access to data related to data breaches via the DHHS Office for Civil Rights breach portal. The recent JAMA Article published in 2018 reviewed this data and showed that hacking and IT incidents have not become the number one breach type. This data is not able to be further classified by what type of hacking or IT incident, such as malware or ransomware attack. There are also limitations on this data set because it only contains incidents that were reported due to data breach. The studies conducted as part of this project identified cyber attack cases where no breach was reported, and therefore the breach data is not inclusive of all malware attacks seen on healthcare providers.

In addition to existing data being hard to access, the healthcare industry is also relatively secretive regarding their attacks. As seen in Study 1 where only 49 malware attacks were located in publicly reported information, based on existing statistics we know this number is an extremely low estimate. With my own experience as an emergency management employee of a healthcare organization during malware attack, administrators were very reticent about letting the public know they were under attack. They expressed concern that patients would worry about their safety when coming in for surgeries or that patients would unnecessarily be concerned with their data privacy. This sentiment was also noted during interviews in Study 2. Healthcare Organizations have both an ethical obligation to protect patients as well as a legal obligation to protect patients' data. An admission of a cyberattack could potentially be an

admission to breaking either or both of these professional obligations. In order for healthcare to be as prepared as they need to be for cybersecurity incidents, it is imperative that individuals in the field of emergency management, safety, and information technology have accurate data that represents the risks these threats pose to healthcare. With accurate and complete information, they can more precisely classify cyber threats to their organizations on their risk assessments and dedicate the needed resources to securing their digital environment.

Another point that was made within this research project is the potential cyberattacks have to impact patient safety, both directly and indirectly. During one of the global malware attacks, patient safety was determined to have been directly put at risk by the effects of the attack (Chappell & Neuman, 2017). These effects included loss of access to patient records and patient care equipment, as well as the diversion of patients en route to impacted hospitals being sent further away and delaying the medical care they required. While limited data currently exists in the academic arena, the healthcare and emergency management fields all agree cyberattacks have the potential to negatively impact patient safety (Ayala, 2016; Lachance, 2016; Barnett, Snell, Lord, Jenkins, Terbush, & Burke, 2013). Stakeholders in Study 2 identified potential for patient care impact during these events, however they were quick to say they did not see a negative patient impact. One potential explanation for this is that while the network is down so too is the error reporting within electronic medical records. Another potential explanation for this is a legal requirement to keep the information confidential. Multiple stakeholders asked during the interviews if their organization had given legal clearance to discuss their facilities attack. So although they did not report a negative patient impact, there is still the potential that it existed.

There is also literature that suggests the potential for active medical devices on the network to become victims of cyberattack (Ayala, 2016; TrapX Labs, 2015). One of these reports reviews case studies where hackers used medical devices to gain access to a network

(TrapX Labs, 2015). While this report does not show evidence hackers used active medical devices to alter patient care, it does show hackers have the ability to remotely gain access to these devices. The other report goes more in detail about how hackers could potentially use this access to hold patient's lives on the line in exchange for ransom rather than locking organizations out of their digital network (Ayala, 2016). A more common concern regarding cyberattacks and patient safety is the reliability of health data being reported by patient care equipment. Stakeholders in Study 2 expressed a concern their organization and providers had during their attack to ensure all health data was accurately being relayed from one digital platform to another. Patient care can be put at risk without access to up to date patient histories and records (Lachance, 2016).

This threat also has the ability to impact patient health through the hospital environment. One of the organizations that participated in Study 2 saw impacts to their HVAC systems. They were forced to manually monitor air flow and temperature around their facility. If they had been unable to keep safe temperature and air quality control, the facility would have been forced to evacuate their patients. As seen in extreme weather conditions, such as Hurricanes Katrina, and Sandy, evacuation of a hospital can be a complex task requiring coordination between large amounts of staff and resources (Adalja, Watson, Bouri, Minton, Morhard, & Toner, 2014; NPR, 2013). Another of the organizations interviewed in Study 2 reported seeing impacts to their security cameras. Due to their inability to visually monitor their entrances and exits, the facility was forced to go in to lockdown and had to increase security presence. If someone with ill intent were to enter the hospital during security downtime due to a cyberevent there is the potential in that scenario as well for patients or visitors of the facility to be injured.

The final point emphasized across this research project is the healthcare field remains vulnerable to cyberattack and needs more efforts for preparedness and security (Kasumov, 2018; Kruse et al., 2017). This industry lags behind other industries in cybersecurity, with many

organizations having out of date cybersecurity systems and not enough training for staff on safe cyber practices (Kruse et al., 2017). Even though healthcare has become the number one targeted industry for cyberattack, they only spend about half as much as other sectors on securing their digital platforms (Silverman, 2018). There has been a 50% decrease in funding for federal hospital emergency preparedness funding over the last 15 years (Watson, Watson, & Sell, 2017). There is a need for sustained funding to assist in healthcare's overall emergency preparedness needs. However, federal funding is only meant to serve as supplemental funding for emergency preparedness. Healthcare is now the second largest sector of the U.S. economy and they should be designating funds in their budgets to improve both safety and emergency management as well as cybersecurity (Silverman, 2018). As the industry expands delivery of care to more digital platforms, healthcare organizations need to make a more concerted effort to secure patient privacy and ensure safe provision of care.

Future Research & Conclusions

With the increased trend in attack occurrence, there seems to be an increase in the number of articles related to this topic. A systematic review published in 2016 included 19 articles from 2008 and 2015, whereas a systematic review published in 2017 included 31 articles the majority of which were published in 2016. However, many of these articles are still news articles rather than academic articles. There is literature related to cybersecurity issues in information technology literature as well as some literature within cyber insurance literature. Both of these literature categories fail to focus on what the disaster recovery cycle at an organizational looks like during cyberattacks or how this threat compares to other threats against healthcare.

This research project served as an exploratory study in to the new and emerging field of cyber threats against healthcare organizations. The studies within this project focused on providing novel data related to the trends, impacts, response, mitigation, and preparation

specifically related to malware attacks against healthcare at the organizational level. The data collected in this project provided a descriptive overview of the topic, but future research is needed on the topic to fully define the risk cyber threats are to the healthcare industry.

A more systematic approach to collecting attack data is necessary to complete a thorough risk assessment for the healthcare industry. As recommended above, a public data depository for cyberattacks, similar to the Department of Health and Human Services Data Breath Portal, would be an excellent answer for healthcare providers. This would allow any individual in the healthcare field to access data and make determinations on their organization's risk based on certain characteristics such as size of facility and geographic location. This database would also house information regarding the impact of each attach, similar to the DHHS database displaying number of individuals impacted. One suggestion on how to accomplish this is a federal regulation similar to the DHHS requirement for providers to report data breaches to the Office for Civil Rights. While this rule leaves reporting ultimately up to the provider to determine whether a breach occurred, due to HIPAA laws and the potential for liability it seems many providers do report. A ruling to develop a reporting requirement would be a push for healthcare providers to make more information on cyberattacks public. Again, this information could be used by healthcare organizations to complete a more accurate risk assessment.

Another future area key to public health research is more evidence-based projects looking at the effects of cyberattacks on patient safety. There is a lot of speculation on potential and determination from previous attacks that patient safety was put at risk, but there are not studies who look at this from a research perspective. Other research could be completed looking at what else within a hospital could be potentially impacted by cyberattacks. This study showed an example of an HVAC system and a security system being impacted, but what other environmental control or safety systems are on a network that could be impacted. There is talk

within the healthcare community that elevators have been hacked in to and stopped, but this is not in the research literature. Quantitative research studies would be key to giving hospital stakeholders the data they need to convince administrators to make system security and preparedness improvements.

Equally important to having data to convince decision makers to act, is understanding the difference of perspectives across departments. A few perspective differences were noted within interviews of Study 2 between the stakeholder departments. These differences were meant to be explored as part of the original objective of Study 3; however the IT group declined to participate and therefore the sample size was not large enough for comparison. This is a research area that is important to examine as knowledge of these differences could be used to get all stakeholders across the organization to agree on best approaches for improved preparedness.

Cyber threats to healthcare are not going to dissipate any time in the near future. A publication from the American Public Health Association estimates over the next five years cyberattacks will cost our nation's healthcare system $305 billion in revenue and will affect 1 in every 13 patients (Krisberg, 2017). Hospitals are a major part to our nation's response network and they are tasked with serving their communities (Barnett et al., 2013). During emergencies, hospitals must be able to safely care for patients on hand as well as handle a surge coming from within their community. Data collected in this research project shows cyberattacks are unlike any hazard or emergency the healthcare industry has faced to date. The impacts of this type of event have the ability to completely shut down an organizations digital network. These events can also last much longer than normal healthcare emergency situations. Healthcare organizations need to expand their emergency operating procedures to include cyberattack. Many of the participants in this study identified the need for healthcare organizations to develop a supplementary plan for cyber threats due to their variance from the all-hazards response and

recovery. Data reports show that despite a clear threat to healthcare and patient safety, the health sector remains vulnerable to attack (Kruse et al., 2017). It is imperative that healthcare organizations heed this call to action to better prepare their organizations to handle this new hazard to ensuring their ability to provide access to safe patient care.

References

Adalja, A.A., Watson, M., Bouri, N., Minton, K., Morhard, R.C., & Toner, E.S. (2014). Absorbing citywide patient surge during Hurricane Sandy: A case study in accommodating multiple hospital evacuations. *Ann Emerg Med*. 64(1):66-73.

Adefala, L. (2018, Mar 6). Healthcare experiences twice the number of cyber attacks as other industries. CSO. Retrieved from https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

Ayala, L. (2016). Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention. Berkeley: Apress.

Barnett, D.J., Snell, T.K., Lord, R.K., Jenkins, C.J., Terbush, J.W., & Burke, T.A. (2013). Cyber security threats to public health. *World Med Health Policy*, 5(1), 37-46.

Cagliuso, N. V. (2014a). Stakeholders' experiences with US hospital emergency preparedness: Part 1. *J Bus Contin Emer Plan*, 8(2), 156-168.

Cagliuso, N. V. (2014b). Stakeholders' experiences with US hospital emergency preparedness: Part 2. *J Bus Contin Emer Plan* , 8(3), 263-279.

Centers for Disease Control and Prevention (CDC). (2014). Disaster Preparedness and Response: Complete Course. Facilitator guide, first edition. Atlanta (GA): CDC. Retrieved from https://www.cdc.gov/nceh/hsb/disaster/Facilitator_Guide.pdf

Chappell, B. and Neuman, S. (2017, Dec 19). U.S. says North Korea 'directly responsible' for wannacry ransomware attack. *NPR*. Retrieved from https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

Columbus, L. (2018, Oct 14). The current state of cybersecurity shows now is the time for zero trust. *Forbes*. Retrieved from https://www.forbes.com/sites/louiscolumbus/2018/10/14/the-current-state-of-cybersecurity-shows-now-is-the-time-for-zero-trust/#342e11da5f15

HIMSS North America (2018). 2018 HIMSS cybersecurity survey. Retrieved from https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf

Kasumov, A. (2018, Jul 17). Cyberattacks on health-care providers are up in recent months. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2018-07-17/cyberattacks-on-health-care-providers-are-up-in-recent-months

Krisberg, K. (2017). Cybersecurity: Public health increasingly facing threats. *The Nation's Health,* 107 (8), 1195.

Kruse, C.S., Frederick, B., Jacobson, T., & Monticone, D.K. (2017). Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care,* 25, 1-10.

Lachance, N. (2016 Apr 1). Malware attacks on hospitals put patients at risk. NPR. Retrieved from https://www.npr.org/sections/alltechconsidered/2016/04/01/472693703/malware-attacks-on-hospitals-put-patients-at-risk

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C.S. (2016). Cyber threats to health information systems: a systemic review. *Technol Health Care*, 24, 1-9.

NPR.(2013, Sept 10). During Katrina, 'Memorial' doctors chose who lived, who died. *NPR*. Retrieved from: https://www.npr.org/2013/09/10/220687231/during-katrina-memorial-doctors-chose-who-lived-who-died

Radke, B.A., Waters, M.J., Cleary, J.C., Evans, D., & Kittle, C. (2016, July 18). Ransomware rises among hospitals. Lexology. Retrieved from http://www.lexology.com/library/detail.aspx?g=8f3d29a5-2f87-42b8-ada1-54a109e38b3f

Silverman, L. (2018 Oct 16). How cyberhardening can reduce risk to the entire medical community. Becker's Hospital Review. Retrieved from https://www.beckershospitalreview.com/cybersecurity/how-cyberhardening-can-reduce-risk-to-the-entire-medical-community.html

TrapX Labs. (2015). Anatomy of an attack: MEDJACK [Medical Device Hijack]. *TrapX Security*. Retrieved from http://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf

United States Department of Health and Human Services Office for Civil Rights. (2016). *Breaches affecting 500 or more individuals* [data file]. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Winton, R. (2016, Feb 18). Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. *Los Angeles Times*. Retrieved from http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Yao, M. (2017, Apr 14). Your electronic medical records could be worth $1000 to hackers. *Forbes.* Retrieved from https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#49f5bec550cf